



Crown
Commercial
Service

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

Part B: Terms and conditions

Schedule 1: Services

Schedule 2: Call-Off Contract charges

Schedule 3: Collaboration agreement

Schedule 4: Alternative clauses

Schedule 5: Not Used

Schedule 6: Glossary and interpretations

Schedule 7: UK GDPR Information

Schedule 8: Security Schedule

Annex 1: Processing Personal Data

Annex 2: Joint Controller Agreement

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	<div></div> <div></div> <div></div>
Call-Off Contract reference	WP2149
Call-Off Contract title	Fraud Risk Engine & Case Management System
Call-Off Contract description	Integrated Fraud Risk Engine and Case Management System solution that will help detect and combat fraudulent activity.
Start date	07th November 2023
Expiry date	6th November 2026
Call-Off Contract value	up to £8,650,000.00 (Ex VAT)
Charging method	<p>License Fees to be paid up front annually from the start of the contract.</p> <p>Implementation Fee to be paid up front from the start of the contract.</p> <p>All other Charges become due following satisfactory delivery of pre-agreed certified products and deliverables.</p> <p>The Supplier will issue valid electronic invoices monthly in arrears.</p>

Purchase order number	To be confirmed
------------------------------	-----------------

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	Government Digital Services The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS
To the Supplier	Synectics Solutions Limited 01782 664000 Synectics House, the Brampton Newcastle-under-Lyme Staffordshire ST5 0QY Company number: 02685135
Together the 'Parties'	

Principal contact details

For the Buyer:

For the Supplier:

Call-Off Contract term

Start date	This Call-Off Contract Starts on 07th November 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 90 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> <p>If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance:</p> <p>https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service</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> <ul style="list-style-type: none"> • Lot 2: Cloud software
G-Cloud Services required	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:</p> <p>To provide integrated fraud risk engine, case management and document sharing tool, through commercial off the shelf products SIRA, Precision and Orion.</p>

	<div data-bbox="737 159 1168 248" data-label="Text"> <p>_____</p> <p>_____</p> </div> <div data-bbox="737 257 1382 365" data-label="Text"> <p>Service Description: https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/795098379878411</p> </div> <div data-bbox="737 376 1382 568" data-label="Text"> <p>Service Definition: https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-13/documents/700774/795098379878411-service-definition-document-2022-05-04-1259.pdf</p> </div> <div data-bbox="737 728 1382 797" data-label="Text"> <p>https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/468907505575280</p> </div> <div data-bbox="737 810 1382 1003" data-label="Text"> <p>Service Definition: https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-13/documents/700774/468907505575280-service-definition-document-2022-05-04-1125.pdf</p> </div> <div data-bbox="737 1014 1168 1153" data-label="Text"> <p>_____</p> <p>_____</p> <p>_____</p> </div> <div data-bbox="737 1162 1382 1232" data-label="Text"> <p>https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/765818033171027</p> </div> <div data-bbox="737 1245 1382 1438" data-label="Text"> <p>Service Definition: https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-13/documents/700774/765818033171027-service-definition-document-2022-05-04-1141.pdf</p> </div> <div data-bbox="588 1467 1294 1538" data-label="Text"> <p>To provide Services in accordance with Schedule 1 of this Call-Off Contract and appendices.</p> </div> <div data-bbox="588 1570 1303 1641" data-label="Text"> <p>To provide Services in accordance with clarifications obtained through the request for clarifications process.</p> </div> <div data-bbox="588 1673 1390 1787" data-label="Text"> <p>There is no guarantee to the Supplier of volume of Services required and the Buyer may increase or decrease the volume of Services to meet its flexible requirements.</p> </div>
Additional Services	Not applicable

Location	The Services will be provided remotely.
Quality Standards	The quality standards required for this Call-Off Contract are as detailed within Schedule 1 of this Call-Off Contract and appendices.
Technical & Security Standards:	<p>All GOV.UK data must be stored and processed on systems hosted in the UK.</p> <p>The Supplier must have relevant user authentication and security and authentication systems in place such as SSO and MFA.</p> <p>The supplier must follow where applicable:</p> <ul style="list-style-type: none"> • The Government Technology Code of Practice https://www.gov.uk/guidance/the-technology-code-of-practice • The Government Service Standard and Service Manual https://www.gov.uk/service-manual/service-standard • <u>Government Cyber Security Policy</u> • NCSC Cyber Assessment Framework Guidance https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework • NCSC guidance https://www.ncsc.gov.uk/section/advice-guidance/all-topics • Government Functional Security Standard No.7 https://www.gov.uk/government/publications/government-functional-standard-govs-007-security • NCSC Cloud Security Principles; https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles • Cyber Essentials plus certification

	<ul style="list-style-type: none"> • ISO 27001 • The Supplier to evidence their resources are cleared to SC clearance level. • Other requirements stated in the Request for Clarification Documents including but not limited to the document WP2149_Fraud Risk Engine & Case Management System_RFC Request for Clarification.
Service level agreement:	<p>The service level and availability criteria required for this Call-Off Contract are:</p> <ul style="list-style-type: none"> • The solution must be able to perform a risk evaluation within 100ms for 99.99% of cases. • The solution must be able to scale to 4000 risk evaluations per second. • The solution must be able to scale at the speed of 4 risk evaluations per second, per second (From 0 r/s to 4000 r/s in 16 minutes 40 seconds). • The solution must ensure that 95% of user-facing requests are served within 1 second [Case Management, Document Sharing, Data Browsing] • The solution must meet the availability expectation minimum of 99.9%. <p>Further service level and availability criteria required for this Call-Off Contract are within the Service Descriptions and Service Definition Documents. Should a conflict arise between the service level requirements stated in this Call-Off Contract and those in the Service Description or Service Definition Documents, this Call-Off contract shall take precedence.</p> <p>The Supplier will engage in performance management reviews as required by the Buyer. Frequency; Initial session; monthly with agreed timelines thereafter.</p>
Onboarding	<p>The onboarding plan for this Call-Off Contract is found in the Service Descriptions and Service Definitions and Supplier clarification responses.</p>

Offboarding	The offboarding plan for this Call-Off Contract is found in the Service Descriptions and Service Definitions and Supplier clarification responses.
Collaboration agreement	Not used.
Limit on Parties' liability	<p>Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £1,000,000 per year.</p> <p>The total liability of the Supplier during each Year for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed £1,000,000 or 125% of the Charges paid and/or committed to be paid by the Buyer to the Supplier for that Year (whichever is the greater).</p> <p>The total liability of the Supplier during each Year for all other Defaults will not exceed the greater of £1,000,000 or 125% of the Charges paid and/or committed to be paid by the Buyer to the Supplier for that Year.</p>
Insurance	<p>The 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 • Data Protection and Cyber Security Protection Insurance

Buyer's responsibilities	The Buyer is responsible for granting the relevant access to data required under this requirement.
Buyer's equipment	<p>The Buyer's equipment to be used with this Call-Off Contract includes:</p> <p>To be confirmed.</p>

Supplier's information

Subcontractors or partners	<p>The following is a list of the Supplier's Subcontractors or Partners: Not applicable.</p> <p>If the Supplier is to rely upon any subprocessors, the Supplier must submit a clear statement of intent to the Buyer for their acceptance.</p>
-----------------------------------	--

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 BACS.</p> <p>The Supplier will issue valid electronic invoices monthly in arrears.</p> <p>The Supplier will send reporting data via .CSV file as well as the PDF invoice so invoices can be automatically reconciled by GDS systems.</p>
-----------------------	--

Payment profile	<p>The payment profile for this Call-Off Contract is monthly in arrears.</p> <p>A PO will be raised (if applicable) once the Call-Off Contract has been signed. The PO is a vehicle for payment and not a firm commitment of spend.</p>
Invoice details	<p>The Supplier will issue electronic invoices monthly in arrears. 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>[REDACTED]</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> <p>[REDACTED]</p>
Invoice information required	<p>All invoices must include the contract reference WP2149 and Purchase Order Number.</p> <p>Each invoice shall be accompanied by a breakdown of the deliverables and services, quantity thereof, applicable unit charges and total charge for the invoice period, in sufficient detail to enable the Customer to validate the invoice.</p> <p>The Supplier will send reporting data via .CSV file as well as the PDF invoice so invoices can be automatically reconciled by GDS systems - see CSV template attached to the email.</p>

Invoice frequency	Invoice will be sent to the Buyer monthly in arrears.
Call-Off Contract value	The total value of this Call-Off Contract is up to £8,650,000.00 (ex VAT).
Call-Off Contract charges	The Charges are as per the Supplier's pricing document in 'Schedule 2 Call-Off Contract charges' as per the Supplier's response to the Request for Clarification.

Performance of the Service	<p>This Call-Off Contract will include the following implementation plan, onboarding, exit / offboarding plans and milestones to provide the Services:</p> <ul style="list-style-type: none"> • As required by Schedule 1 and Appendices • Supplier to provide implementation plan, onboarding plan, exit / offboarding plan.
Guarantee	Not applicable.

Warranties, representations	<p>In addition to the incorporated Framework Agreement clause 2.3, the Supplier warrants and represents to the Buyer that:</p> <p>Not applicable.</p>
Supplemental requirements in addition to the Call-Off terms	Not used.
Alternative clauses	<p>These Alternative Clauses, which have been selected from Schedule 4, will apply:</p> <p>Not applicable.</p>
Buyer specific amendments to/refinements of the Call-Off Contract terms	<p>Within the scope of the Call-Off Contract, the Supplier will agree to and comply with the Security Management Schedule (Supplier-led Assurance).</p> <ol style="list-style-type: none"> 1. The Supplier shall engage and collaborate with GDS Security Working Group reviews led by Digital Identity security leads. 2. The Supplier shall comply with the Security standards and requirements set out in Schedule 8. 3. The Supplier acknowledges and agrees: <ol style="list-style-type: none"> a. that the Buyer intends to use the Services as a component of a cross-government digital identity solution which will enable a user to prove their identity for the purpose of accessing certain government services;

	<p>b. The government services which use the Buyer's digital identity solution will be relying parties ("Relying Parties"); and</p> <p>c. any loss suffered by a Relying Party as a result the Supplier's Default in its obligations is deemed to be suffered by and recoverable by GDS as a direct loss under this Call Off Contract.</p>
Personal Data and Data Subjects	Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1
Intellectual Property	All Intellectual Property Rights in the G-Cloud Services as detailed in part A of the Order Form belong to the Supplier.
Social Value	To be delivered as per the Suppliers response to the WP2149 - Fraud Risk Engine & Case Management System - RFC Request for Clarification.

Additional Buyer terms

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. Security

- 2.1. The Supplier shall engage and collaborate with GDS Security Working Group reviews led by Digital Identity security leads.
- 2.2. The Supplier shall comply with Schedule 8 - Security Schedule.
- 2.3. The Supplier shall provide a completed Security Management Plan within 20 Working days of a signed contract as set out in the Security Schedule 13 (4).

3. Background to the agreement

- 3.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13.
- 3.2 The Buyer provided an Order Form for Services to the Supplier.

Signed	Supplier	Buyer
Name	Marian Humphreys	WILLIAM MAY
Title	Legal Director	COMMERCIAL DIRECTOR
Signature		
Date	3 November 2023	08 November 2023

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) - NOT USED
- 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:

1. a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
2. a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'
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
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.
4. The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.
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:

1. rights granted to the Buyer under this Call-Off Contract
2. Supplier's performance of the Services
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:

1. modify the relevant part of the Services without reducing its functionality or performance
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
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:

1. the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
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:

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
2. return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
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
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
5. work with the Buyer on any ongoing work
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

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.
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.

- 1.3. 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.
- 1.4. 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.
- 1.1. The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
 - 1.1.1. its failure to comply with the provisions of this clause
 - 1.1.1. any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
- 1.2. The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
- 1.3. 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

SIRA

Service Description:

<https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/795098379878411>

Service Definition:

<https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-13/documents/700774/795098379878411-service-definition-document-2022-05-04-1259.pdf>

ORION

Service Description:

<https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/468907505575280>

Service Definition:

<https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-13/documents/700774/468907505575280-service-definition-document-2022-05-04-1125.pdf>

PRECISION

Service Description:

<https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/765818033171027>

Service Definition:

<https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-13/documents/700774/765818033171027-service-definition-document-2022-05-04-1141.pdf>

Appendices that further describe the required Services and are part of this Call-Off Contract:

Schedule_1_Appendix_A_WP2149_Fraud_Risk_Engine_& Case_Management_System_RFC

Schedule_1_Appendix B_WP2149_Fraud_Risk_Engine_& Case_Management_System_Annex
C_Technical_and_Non_Technical_Requirements.xlsx

The Appendices are considered to be clauses of the Call Off Contract for the purpose of clause 8.3 of the Framework Agreement shall take precedence over the Service Descriptions to the extent of any inconsistency.

Schedule 2: Call-Off Contract charges

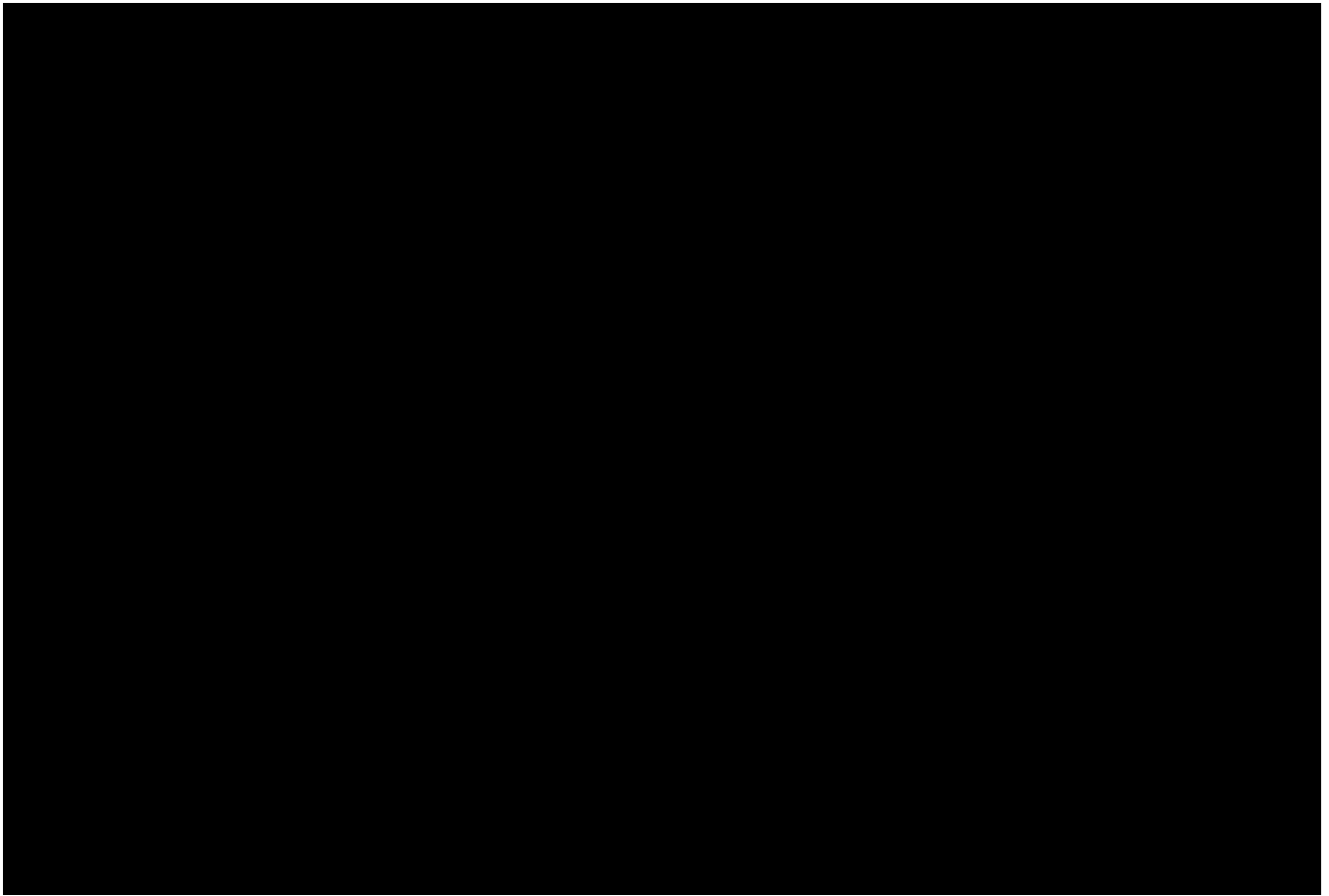
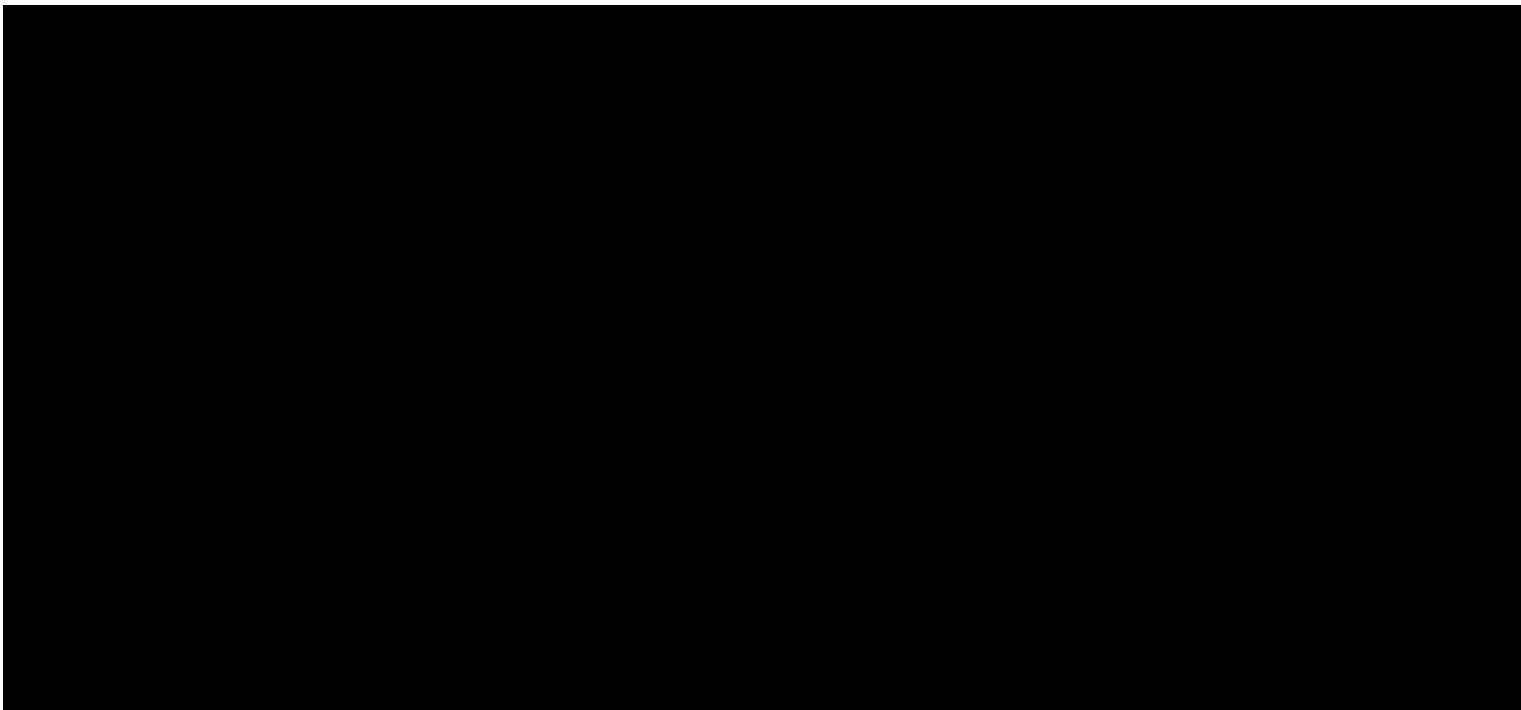
A large rectangular area that has been completely redacted with a solid black fill, obscuring all content within its boundaries.

Table A

A large rectangular area that has been completely redacted with a solid black fill, obscuring all content within its boundaries.

Schedule 3: Not Used

Schedule 4: Alternative clauses

1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

2.1 The Customer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 15.1 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.1.

2.1.6 References to "tort" will be replaced with "delict" throughout

2.2 The Customer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

- Employment (Northern Ireland) Order 2002
- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988
- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
- Equal Pay Act (Northern Ireland) 1970

- Disability Discrimination Act 1995
- Race Relations (Northern Ireland) Order 1997
- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996
- Employment Equality (Age) Regulations (Northern Ireland) 2006
- Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
- Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- The Disability Discrimination (Northern Ireland) Order 2006
- The Employment Relations (Northern Ireland) Order 2004
- Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
- Employment Relations (Northern Ireland) Order 2004 • Work and Families (Northern Ireland) Order 2006

and will use his best endeavours to ensure that in his employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract he promotes equality of treatment and opportunity between:

- a. persons of different religious beliefs or political opinions
- b. men and women or married and unmarried persons
- c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
- d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
- e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
- f. persons of different ages
- g. persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Customer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

- a. the issue of written instructions to staff and other relevant persons
- b. the appointment or designation of a senior manager with responsibility for equal opportunities
- c. training of all staff and other relevant persons in equal opportunities and harassment matters
- d. the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Customer as soon as possible in the event of:

- A. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or
- B. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Period by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Customer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Customer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Customer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Customer in relation to same.

2.6 Health and safety

2.6.1 The Supplier will promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Customer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Customer premises, the Supplier will comply with any health and safety measures implemented by the Customer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Customer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Customer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Customer on request.

2.7 Criminal damage

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Customer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).

2.7.2 If during the Call-Off Contract Period any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation

under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Customer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Customer's cost and the Supplier will (at no additional cost to the Customer) provide any help the Customer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5: - Not Used

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	<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 Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans

Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.13 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or

	defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.

UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	Not required.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.

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

Insolvency event	Can be: <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	Intellectual Property Rights are: <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 and which are specifically agreed in writing by the parties to be Project Specific 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-controls/when-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: UK GDPR Information

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

Annex 1: Processing Personal Data

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

1.1 The contact details of the Buyer's Data Protection Officer are:

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

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

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

Description	Details
Identity of Controller for each Category of Personal Data	The Buyer is the Controller. The Supplier is the Processor. The Parties acknowledge that for the purposes of the Data Protection Legislation, Buyer is the Controller and the Supplier is the Processor of the Personal Data recorded below.
Duration of the Processing	<i>For the Duration of the contract between the Parties</i>

Nature and purposes of the Processing	Data is processed for the purposes of a Fraud Risk Engine and Case Management System which supports the GOV.UK One Login programme.
Type of Personal Data	<ul style="list-style-type: none"> <i>Personal data of the citizen which is received from the Identity Verification process which includes and not limited to; name, address, date of birth, telephone number IP address, Gender identity, NI number, images, biometric identity data,</i>

Categories of Data Subject	<i>Citizens Personal Data, Administrators of the system.</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	<i>Prior to the end of the contract (and as part of the Exit plan agreement) the Controller will set out timelines and for which the processor will be required to delete/destroy relevant data sets as determined by the Controller. Following such deletion/destruction of data, a relevant assurance statement will be provided by the Processor to the Controller. Relevant data controls will be applied no later than a 6 month period following contract end.</i>

Schedule 8 - Security Schedule:

(Security Management: Supplier-led Assurance)

Contents

1	Buyer Options	1
2	Definitions	1
3	Introduction	12
4	Principles of security	13
5	Security requirements	13
6	Buyer to proceed	13
7	Supplier confirmation	14
8	Governance	14
9	Personnel	15
10	Sub-contractors	16
11	Supplier Information Management System	17
12	Certification Requirements	17
13	Security Management Plan	19
14	Monitoring and updating Security Management Plan	21
15	Review and approval of Security Management Plan	22
16	Changes to the Supplier Information Management System	23
17	Remediation Action Plan	24
18	Independent Security Adviser	25
19	Withholding of Charges	27
20	Access to Buyer System	28
1.	Location	29
2.	Vetting, Training and Staff Access	31
3.	End-user Devices	32
4.	Hardware and software support	33
5.	Encryption	34
6.	Email	35
7.	DNS	35
8.	Malicious Software	35
9.	Vulnerabilities	36
10.	Security testing	37
11.	Access Control	41
12.	Event logging and protective monitoring	42
13.	Audit rights	43
14.	Breach of Security	45
15.	Return and Deletion of Buyer Data	46
1.	Secure Software Development by Design	48
2.	Secure Architecture	49

3.	Code Repository and Deployment Pipeline	49
4.	Development and Testing Data	49
5.	Code Reviews	49
6.	Third-party Software	50
7.	Third-party Software Modules	50

1 Buyer Options

- 1.1 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

Locations (see paragraph 1 of the Security Requirements)		
The Supplier and Sub-Contractors may store, access or Process Buyer Data in:	the United Kingdom only	<input checked="" type="checkbox"/>
	the United Kingdom and European Economic Area only	<input type="checkbox"/>
	anywhere in the world not prohibited by the Buyer	<input type="checkbox"/>
Support Locations (see paragraph 1 of the Security Requirements)		
The Supplier and Sub-Contractors may operate Support Locations in:	the United Kingdom only	<input checked="" type="checkbox"/>
	the United Kingdom and European Economic Area only	<input type="checkbox"/>
	anywhere in the world not prohibited by the Buyer	<input type="checkbox"/>
Locations for Development Activity (see paragraph 1 of the Security Requirements)		
The Supplier and Sub-Contractors may undertake Development Activity in:	the United Kingdom only	<input checked="" type="checkbox"/>
	the United Kingdom and European Economic Area only	<input type="checkbox"/>
	anywhere in the world not prohibited by the Buyer	<input type="checkbox"/>

2 Definitions

“Anti-virus Software”	<p>means software that:</p> <ul style="list-style-type: none"> (a) protects the Supplier Information Management System from the possible introduction of Malicious Software; (b) scans for and identifies possible Malicious Software in the Supplier Information Management System; (c) if Malicious Software is detected in the Supplier Information Management System, so far as possible:
------------------------------	--

	<p>(i) prevents the harmful effects of the Malicious Software; and</p> <p>(ii) removes the Malicious Software from the Supplier Information Management System;</p>
"Buyer Data"	<p>as defined in this Schedule 1 (Definitions) and, for the avoidance of doubt, shall include any meta data relating to categories of data referred to in paragraphs (a) or (b), the Code and any meta data relating to the Code.</p> <ul style="list-style-type: none"> Data categories described within the Data Processing Schedule
"Buyer Data Register"	<p>means the register of all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer, produced and maintained in accordance with paragraph 15 of the Security Requirements;</p>
"Buyer Premises"	<p>as defined in Schedule 1 (Definitions);</p>
"Buyer System"	<p>as defined in Schedule 1 (Definitions);</p>
"Breach Action Plan"	<p>means a plan prepared under paragraph 14.3 of the Security Requirements addressing any Breach of Security;</p>
"Breach of Security"	<p>for the purposes of this Security Schedule, means the occurrence of:</p> <p>(a) any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Contract, including the Buyer Data and the Code;</p> <p>(d) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in connection with this Contract, including the Buyer Data and the Code; and/or</p> <p>(e) any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements;</p> <p>(f) the installation of Malicious Software in the:</p> <p>(i) Supplier Information Management System;</p> <p>(ii) Development Environment; or</p> <p>(iii) Developed System;</p>

	<p>(g) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the:</p> <p>(i) Supplier Information Management System;</p> <p>(ii) Development Environment; or</p> <p>(iii) Developed System; and</p> <p>(h) includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:</p> <p>(i) was part of a wider effort to access information and communications technology by or on behalf of Central Government Bodies; or</p> <p>(ii) was undertaken, or directed by, a state other than the United Kingdom</p>
“Certification Requirements”	means the requirements set out in paragraph 12.3.
“CHECK Scheme”	means the NCSC’s scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks
“CHECK Service Provider”	<p>means a company which, under the CHECK Scheme:</p> <p>(a) has been certified by the National Cyber Security Centre;</p> <p>(b) holds “Green Light” status; and</p> <p>(c) is authorised to provide the IT Health Check services required by paragraph 10 of the Security Requirements;</p>
“Code”	<p>means, in respect of the Developed System:</p> <p>(a) the Source code;</p> <p>(b) the Object code;</p> <p>(c) third-party components, including third-party coding frameworks and libraries; and</p> <p>(d) all supporting documentation.</p>
“Code Review”	<p>means a periodic review of the Code by manual or automated means to:</p> <p>(a) identify and fix any bugs; and</p> <p>(b) ensure the Code complies with</p>

	<p>(i) the requirements of this Security Schedule ; and</p> <p>(ii) the Secure Development Guidance;</p>
“Code Review Plan”	means the document agreed with the Buyer under paragraph 5.2 of the Security Requirements setting out the requirements for, and frequency of, Code Reviews;
“Code Review Report”	means a report setting out the findings of a Code Review;
“Cyber Essentials”	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Plus”	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Scheme”	means the Cyber Essentials scheme operated by the National Cyber Security Centre;
“Developed System”	<p>means any software or system that the Supplier will develop under this Contract either:</p> <p>(a) as part of the Services; or</p> <p>(b) to create or modify Software to:</p> <p>(i) provide the Services; or</p> <p>(ii) Process Buyer Data,;</p>
“Development Activity”	<p>means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including:</p> <p>(a) coding;</p> <p>(b) testing;</p> <p>(c) code storage; and</p> <p>(d) deployment.</p>
“Development Environment”	means any information and communications technology system and the Sites forming part of the Supplier Information Management System that the Supplier or its Sub-contractors will use to provide the Development Activity;
“EEA”	means the European Economic Area;
“End-user Device”	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services.
“Email Service”	means a service that will send, or can be used to send, emails from the Buyer’s email address or otherwise on behalf of the Buyer;
“Higher Risk Sub-contractor”	means a Sub-contractor that Processes Buyer Data, where that data includes either:

	<p>(a) the Personal Data of 1000 or more individuals in aggregate during the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with Clause 4.1(b); or</p> <p>(b) any part of that Buyer Data includes any of the following:</p> <ul style="list-style-type: none"> (i) financial information (including any tax and/or welfare information) relating to any person; (ii) any information relating to actual or alleged criminal offences (including criminal records); (iii) any information relating to children and/or vulnerable persons; (iv) any information relating to social care; (v) any information relating to a person's current or past employment; or (vi) Special Category Personal Data; or <p>(c) the Buyer in its discretion, designates a Sub-contractor as a Higher Risk Sub-Contractor:</p> <ul style="list-style-type: none"> (i) in any procurement document related to this Contract; or (ii) during the Term;
"HMG Baseline Personnel Security Standard"	means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 6.0, May 2018 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf), as that document is updated from time to time;
"Independent Security Adviser"	means the independent and appropriately qualified and experienced security architect or expert appointed under Paragraph 18;
"Information Management System"	means the Supplier Information Management System and the Wider Information Management System;
"IT Health Check"	means testing of the Supplier Information Management System by a CHECK Service Provider;

International Data Transfer Agreement (IDTA's)	Replaces Standard Contract Clauses under UK GDPR for International data transfers/restricted data transfers, and processing of data outside the UK
"Malicious Software"	as defined in Schedule 1 (Definitions);
"Medium Risk Sub-contractor"	<p>means a Sub-contractor that Processes Buyer Data, [where that data</p> <p style="margin-left: 40px;">(a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with Clause 4.1(b); and</p> <p style="margin-left: 40px;">(b) does not include Special Category Personal Data;</p>
"Modules Register"	means the register of Third-party Software Modules required by paragraph 7.2 of the Security Requirements;
"NCSC"	means the National Cyber Security Centre;
"NCSC Cloud Security Principles"	means the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles .
"NCSC Device Guidance"	means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance ;
"NCSC Protecting Bulk Personal Data Guidance"	means the NCSC's document "Protecting Bulk Personal Data", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data
"NCSC Secure Design Principles"	means the NCSC's document "Secure Design Principles", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cyber-security-design-principles .
"OWASP"	means the Open Web Application Security Project Foundation;
"OWASP Secure Coding Practice"	means the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content ;
"OWASP Top Ten"	means the list of the most critical security risks to web applications published annually by OWASP and found at https://owasp.org/www-project-top-ten/ ;
"Privileged User"	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;

“Process”	means any operation performed on data (which includes without limitation, Personal Data), whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data, and “Processing” shall be interpreted accordingly”;
“Prohibited Activity”	means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice;
“Prohibition Notice”	means a notice issued under paragraph 1.8 of the Security Requirements.
“Protective Monitoring System”	means the system implemented by the Supplier and its Sub-contractors under paragraph 12.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code
“Register of Support Locations and Third-Party Tools”	<p>means the part of the Security Management Plan setting out, in respect of Support Locations and Third-Party Tools:</p> <ul style="list-style-type: none"> (a) the nature of the activity performed at the Support Location or by the Third-Party Tool on the Code or the Buyer Data (as applicable); (b) where that activity is performed by individuals, the place or facility from where that activity is performed; and (c) in respect of the entity providing the Support Locations or Third-Party Tools, its: <ul style="list-style-type: none"> (i) full legal name; (ii) trading name (if any) (iii) country of registration; (iv) registration number (if applicable); and (v) registered address.
“Relevant Activities”	means those activities specified in paragraph 1.1 of the Security Requirements.
“Relevant Certifications”	<p>means:</p> <ul style="list-style-type: none"> (a) in the case of the Supplier, any SIMS Sub-contractor and any Sub-contractor that Processes Buyer Data: <ul style="list-style-type: none"> (i) ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider

	<p>certification of compliance with ISO/IEC 27001:2013; and</p> <p>(ii) Cyber Essentials Plus; and</p> <p>(b) for all other Sub-contractors means Cyber Essentials Plus;</p>
“Relevant Convictions”	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences) or any other offences relevant to Services as the Buyer may specify
“Remediation Action Plan”	means the plan prepared by the Supplier in accordance with Paragraph 10.20 to 10.24, addressing the vulnerabilities and findings in a IT Health Check report
“Risk Management Approval Statement”	the statement issued by the Buyer under Paragraph 15.2 following the Buyer-led Assurance of the Supplier Information Management System;
“Secure Development Guidance”	means the Supplier’s secure coding policy required under its ISO27001 Relevant Certification;
“Security Management Plan”	means the document prepared in accordance with the requirements of Paragraph 13 and in the format, and containing the information, specified in Annex 2.
“Security Requirements”	mean the security requirements in Annex 1 to this Security Schedule
“Security Requirements for Development”	means the security requirement Annex 2 to this Security Schedule
"Security Test"	<p>means:</p> <p>(a) an Buyer Security Test;</p> <p>(b) an IT Health Check; or</p> <p>(c) a Supplier Security Test.</p>
"Security Working Group"	means the Board established under Paragraph 8 or Schedule 7 (Governance), as applicable;
“SIMS Sub-contractor”	means a Sub-contractor designated by the Buyer that provides or operates the whole, or a substantial part, of the Supplier Information Management System;
“Sites”	<p>means any premises (including the Buyer Premises, the Supplier’s premises or third-party premises):</p> <p>(a) from, to or at which:</p>

	<ul style="list-style-type: none"> (i) the Services are (or are to be) provided; or (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or <p>(b) where:</p> <ul style="list-style-type: none"> (i) any part of the Supplier System is situated; or (ii) any physical interface with the Buyer System takes place;
“SMP Sub-contractor”	<p>means a Sub-contractor with significant market power, such that:</p> <ul style="list-style-type: none"> (c) they will not contract other than on their own contractual terms; and (d) either: <ul style="list-style-type: none"> (i) there are no other substitutable suppliers of the particular services other than SMP Sub-contractors; or (ii) the Sub-contractor concerned has an effective monopoly on the provision of the Services.
“Statement of Information Risk Appetite”	<p>means the statement provided by the Buyer under Paragraph 7.1 setting out the nature and level of risk that the Supplier accepts from the operation of the Supplier Information Management System.</p>
“Sub-contractor”	<p>as defined in Schedule 1 (Definitions) and includes, for the purposes of this Security Schedule , any individual or entity that:</p> <ul style="list-style-type: none"> (a) forms part of the supply chain of the Supplier; and (b) has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Buyer Data;
“Sub-contractor Personnel”	<p>means:</p> <ul style="list-style-type: none"> (c) any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and (d) engaged in or likely to be engaged in: <ul style="list-style-type: none"> (i) the performance or management of the Services; (ii) or the provision of facilities or services that are necessary for the provision of the Services.

"Sub-contractors' Systems"	<p>means the information and communications technology system used by a Sub-contractor in implementing and performing the Services, including:</p> <ul style="list-style-type: none"> (a) the Software; (b) the Supplier Equipment; (c) configuration and management utilities; (d) calibration and testing tools; (e) and related cabling; but <p>does not include the Buyer System;</p>
"Supplier Information Management System"	<p>means</p> <ul style="list-style-type: none"> (a) the Supplier System; (b) the Sites; (c) any part of the Buyer System the Supplier or any Sub-contractor will use to Process Buyer Data, or provide the Services; and (d) the associated information management system, including all relevant: <ul style="list-style-type: none"> (i) organisational structure diagrams, (ii) controls, (iii) policies, (iv) practices, (v) procedures, (vi) processes; and (vii) resources;
"Supplier Personnel"	as defined in Schedule 1 (Definitions);
"Supplier System"	as defined in Schedule 1 (Definitions);
"Support Location"	means a place or facility where or from which individuals may access or Process the Code or the Buyer Data;
"Support Register"	means the register of all hardware and software used to provide the Services produced and maintained in accordance with paragraph 4 of the Security Requirements.
"Third-party Software Module"	<p>means any module, library or framework that:</p> <ul style="list-style-type: none"> (a) is not produced by the Supplier or a Sub-contractor as part of the Development Activity; and (b) either:

	<p>(i) forms, or will form, part of the Code; or</p> <p>(ii) is, or will be, accessed by the Developed System during its operation.</p>
“Third-party Tool”	means any activity conducted other than by the Supplier during which the Code or the Buyer Data is accessed, analysed or modified or some form of operation is performed on it;
“UKAS”	means the United Kingdom Accreditation Service;
“Wider Information Management System”	<p>means</p> <p>(e) any:</p> <p>(i) information assets,</p> <p>(ii) IT systems,</p> <p>(iii) IT services; or Sites</p> <p>that:</p> <p>(f) the Supplier or any Sub-contractor will use to:</p> <p>(i) Process, or support the Processing of, Buyer Data; or</p> <p>(ii) provide, or support the provision of, the Services; or</p> <p>(g) any IT systems controlled or operated by the Supplier or any Sub-contractor that interface such;</p> <p>together with the associated information management system, including all relevant:</p> <p>(i) organisational structure diagrams,</p> <p>(ii) controls,</p> <p>(iii) policies,</p> <p>(iv) practices,</p> <p>(v) procedures,</p> <p>(vi) processes; and</p> <p>(vii) resources.</p>

3 Introduction

3.1 This Security Schedule sets out:

- (a) the Buyer’s decision on where the Supplier may:
- (i) store, access or process Buyer Data;
 - (ii) undertake the Development Activity;

- (iii) host the Development Environment; and
 - (iv) locate Support Locations,
(in Paragraph 1)
- (b) the principles of security that apply to this Contract (in Paragraph 4);
- (c) the requirement to obtain a Risk Management Approval Statement (in Paragraphs 6 and 15);
- (d) the annual confirmation of compliance to be provided by the Supplier (in Paragraph 7);
- (e) the governance arrangements for security matters, where these are not otherwise specified in Schedule 7 (*Governance*) (in Paragraph 8);
- (f) access to personnel (in Paragraph 9);
- (g) obligations in relation to Sub-contractors (in Paragraph 10);
- (h) the responsibility of the Buyer to determine the Supplier Information Management System that will be subject to Buyer-led Assurance (in Paragraph 11);
- (i) the Certification Requirements (in Paragraph 12);
- (j) the development, monitoring and updating of the Security Management Plan by the Supplier (in Paragraphs 13, 14 and 15);
- (k) the granting by the Buyer of approval for the Supplier to commence:
 - (i) the provision of Services; and/or
 - (ii) Processing Buyer Data (in Paragraph 6);
- (l) the management of changes to the Supplier Information Management System (in Paragraph 16); and
- (m) the Buyer's additional remedies for breach of this Security Schedule), including:
 - (i) the requirement for Remediation Action Plans (in Paragraph 17);
 - (ii) the appointment of Independent Security Advisers (in Paragraph 18); and
 - (iii) the withholding of Charges by the Buyer (in Paragraph 19).

4 Principles of security

4.1 The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data and, consequently, on the security of:

- (a) the Buyer System;
- (b) the Supplier System;
- (c) the Sites;

- (d) the Services; and
 - (e) the Supplier Information Management System.
- 4.2 The Parties shall share information and act in a co-operative manner at all times to further the principles of security in Paragraph 4.1.

5 Security requirements

- 5.1 The Supplier must, unless otherwise agreed in writing with the Buyer:
- (a) comply with the Security Requirements; and
 - (b) subject to Paragraph 5.2, ensure that Sub-contractors comply with the Security Requirements.
- 5.2 Where a Sub-contractor is a SMP Sub-contractor, the Supplier shall:
- (a) use best endeavours to ensure that the SMP Sub-contractor complies with the Security Requirements;
 - (b) document the differences between Security Requirements the obligations that the SMP Sub-contractor is prepared to accept in sufficient detail to allow the Buyer to form an informed view of the risks concerned;
 - (c) take such steps as the Buyer may require to mitigate those risks.
- 5.3 Where the Supplier or any Sub-contractor undertakes Development Activity the Supplier must (where applicable) comply, and ensure that any applicable Sub-contractor complies, with the Security Requirements for Development.

6 Buyer to proceed

- 6.1 Notwithstanding anything in this Contract, the Supplier may not:
- (a) commence the provision of any Services; or
 - (b) Process any Buyer Data using the Supplier Information Management System, unless:
 - (c) the Supplier has, and ensured that Sub-contractors have, obtained the Relevant Certifications under Paragraph 12;
 - (d) the Supplier has completed an IT Health Check in accordance with paragraph 10 of the Security Requirements; and
 - (e) the Buyer has provided a Risk Management Approval Statement under Paragraph 13.

7 Supplier confirmation

- 7.1 The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its [chief executive officer] (or equivalent officer) confirming that, having made due and careful enquiry:
- (a) the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Contract;
 - (b) subject to Paragraph 7.2:
 - (i) it has fully complied with all requirements of this Security Schedule ; and
 - (ii) all Sub-contractors have complied with the requirements of this Security Schedule with which the Supplier is required to ensure they comply;
 - (c) the Supplier considers that its security and risk mitigation procedures remain effective.
- 7.2 Where the Buyer has, in respect of the period covered by the confirmation provided under Paragraph 7.1 agreed in writing that the Supplier need not, or need only partially, comply within any requirement of this Security Schedule :
- (a) the confirmation must include details of the Buyer's agreement; and
 - (b) confirm that the Supplier has fully complied with that modified requirement.
- 7.3 The Supplier must:
- (a) keep and maintain a register setting out all agreements referred to in Paragraph 7.2; and
 - (b) provide a copy of that register to the Buyer on request.

8 Governance

- 8.1 This Paragraph 8 applies where a Security Working Group, or Board (as that term is defined in Schedule 7 (*Governance*) with a similar remit, is not provided for otherwise in this Contract.
- 8.2 The Buyer must establish a Security Working Group on which both the Buyer and the Supplier are represented.
- 8.3 The notice or other document establishing the Security Working Group must set out:
- (a) the Buyer members;
 - (b) the Supplier members;
 - (c) the chairperson of the Security Working Group;
 - (d) the date of the first meeting;
 - (e) the frequency of meetings; and

- (f) the location of meetings
- 8.4 The Security Working Group has oversight of all matters relating to the security of the Buyer Data and the Supplier Information Management System.
- 8.5 The Security Working Group meets:
 - (a) once every Contract Year following the review of the Security Management Plan by the Supplier under Paragraph 14 and before the Buyer has completed its review of the updated Security Management Plan under Paragraph 15; and
 - (b) additionally when required by the Buyer.
- 8.6 The Supplier must ensure that the Supplier Personnel attending each meeting of the Security Working Group:
 - (a) have sufficient knowledge and experience to contribute to the discussion of the matters on the agenda for the meeting;
 - (b) are authorised to make decisions that are binding on the Supplier in respect of those matters, including any decisions that require expenditure or investment by the Supplier; and
 - (c) where relevant to the matters on the agenda for the meeting, include representatives of relevant Sub-contractors.
- 8.7 Any decisions, recommendations or advice of the Security Working Group:
 - (a) are not binding on the Supplier; and
 - (b) do not limit or modify the Supplier's responsibilities under this Security Schedule
- 8.8 Appendix 3 applies to the Security Working Group.

9 Personnel

- 9.1 The Supplier must ensure that at all times it maintains within the Supplier Personnel sufficient numbers of qualified, skilled security professionals to ensure the Supplier complies with the requirements of this Security Schedule.
- 9.2 To facilitate:
 - (a) the Buyer's oversight of the Supplier Information Management System; and
 - (b) the Supplier's design, implementation, operation, management and continual improvement of the Security Management Plan and the security of the Services and Information Management System and otherwise,at reasonable times and on reasonable notice:
 - (c) the Supplier shall provide access to the Supplier Personnel responsible for information assurance; and
 - (d) the Buyer shall provide access to its personnel responsible for information assurance.

10 Sub-contractors

SIMS Sub-contractor

- 10.1 Notwithstanding anything else in this Contract but subject to Paragraph , a SIMS Sub-contractor shall be treated for all purposes as a Key Sub-contractor.
- 10.2 In addition to the obligations imposed by this Contract on Key Sub-contractors, the Supplier must ensure that the Key Subcontract with each SIMS Sub-contractor:
- (a) contains obligations no less onerous on the Key Sub-contractor than those imposed on the Supplier under this Security Schedule ; and
 - (b) provides for the Buyer to perform Buyer-led Assurance of any part of the Supplier Information Management System that the SIMS Sub-contractor provides or operates that is not otherwise subject to Buyer-led Assurance under this Security Schedule).
- 10.3 Where a SIMS Sub-contractor is also a SMP Sub-contractor, the Supplier shall:
- (a) use best endeavours to ensure that the SMP Sub-contractor complies with the requirements of this Contract relating to Key Sub-contractors;
 - (b) document the differences between the Key Sub-contractor obligations imposed by this Contract and the Key Sub-contractor obligations that the SMP Sub-contractor is prepared to accept in sufficient detail to allow the Buyer to form an informed view of the risks concerned;
 - (c) take such steps as the Buyer may require to mitigate those risks.

Sub-contractors

- 10.4 Unless otherwise set out in the table in Appendix 4 (*Sub-contractor Security Requirements and Security Requirements for Development*), the Supplier must ensure that Sub-contractors comply with all Security Requirements and Security Requirements for Development that apply to the activities that the Sub-contractor performs under its Sub-contract with the Supplier.
- 10.5 The Supplier must, before entering into a binding Sub-contract with any Sub-contractor:
- (a) undertake sufficient due diligence of the proposed Sub-contractor to provide reasonable assurance that the proposed Sub-contractor can perform the obligations that this Schedule requires the Supplier ensure that the proposed Sub-contractor performs;
 - (b) keeps adequate records of the due diligence it has undertaken in respect of the proposed Sub-contractors; and
 - (c) provides those records to the Buyer on request.

11 Supplier Information Management System

- 11.1 The Supplier must determine:
- (a) the scope and component parts of the Supplier Information Management System; and

- (b) the boundary between the Supplier Information Management System and the Wider Information Management System.
- 11.2 Before making the determination under Paragraph 11.1, the Supplier must consult with the Buyer and in doing so must provide the Buyer with such documentation and information that the Buyer may require regarding the Wider Information Management System.
- 11.3 The Supplier shall reproduce its determination under Paragraph 11.1 as a diagram documenting the components and systems forming part of the Information Management System and the boundary between the Supplier Information Management System and the Wider Information Management System.
- 11.4 The diagram prepared under Paragraph 11.3 forms part of the Security Management Plan.
- 11.5 Any proposed change to:
 - (a) the component parts of the Supplier Information Management System; or
 - (b) the boundary between the Supplier Information Management System and the Wider Information Management System,is:
 - (a) an Operational Change to which the Change Control Procedure applies;
 - (b) requires approval by the Buyer under Paragraph 16; and
 - (c) the Buyer may require the appointment of an Independent Security Adviser to advise on the proposed change.

12 Certification Requirements

- 12.1 The Supplier shall ensure that, unless otherwise agreed by the Buyer, both:
 - (a) it; and
 - (b) any Sub-contractor,are certified as compliant with the Relevant Certifications, that is to say:
 - (c) in the case of the Supplier, any SIMS Sub-contractor and any Sub-contractor that Processes Buyer Data:
 - (i) ISO/IEC 27001:2013/ 2022 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2022; and
 - (ii) Cyber Essentials Plus; and
 - (d) for all other Sub-contractors, Cyber Essentials Plus.
- 12.2 Unless otherwise agreed by the Buyer, before it begins to provide the Services, the Supplier must provide the Buyer with a copy of:
 - (a) the Relevant Certifications for it and any Sub-contractor; and

- (b) the relevant scope and statement of applicability required under the ISO/IEC 27001:2022 Relevant Certifications.
- 12.3 The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications for it and any Sub-contractor are:
 - (a) currently in effect;
 - (b) cover at least the full scope of the Supplier Information Management System; and
 - (c) are not subject to any condition that may impact the provision of the Services or the Development Activity,

(the “**Certification Requirements**”).
- 12.4 The Supplier must notify the Buyer promptly, and in any event within 3 Working Days, after becoming aware that, in respect of it or any Sub-contractor:
 - (a) a Relevant Certification has been revoked or cancelled by the body that awarded it;
 - (b) a Relevant Certification expired and has not been renewed by the Supplier;
 - (c) a Relevant Certification no longer applies to the full scope of the Supplier Information Management System; or
 - (d) the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a “**Certification Default**”)
- 12.5 Where the Supplier has notified the Buyer of a Certification Default under Paragraph 12.4:
 - (a) the Supplier must, within 10 Working Days of the date in which the Supplier provided notice under Paragraph 12.4 (or such other period as the Parties may agree) provide a draft plan (a “**Certification Rectification Plan**”) to the Buyer setting out:
 - (i) full details of the Certification Default, including a root cause analysis;
 - (ii) the actual and anticipated effects of the Certification Default;
 - (iii) the steps the Supplier and any Sub-contractor to which the Certification Default relates will take to remedy the Certification Default;
 - (b) the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;
 - (c) if the Buyer rejects the Certification Rectification Plan, the Supplier must within 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph 12.5(b) will apply to the re-submitted plan;
 - (d) the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Contract;
 - (e) if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

13 Security Management Plan

Purpose of Security Management Plan

- 13.1 The Buyer may, at any time, provide the Supplier with a Statement of Risk Appetite.
- 13.2 The Supplier must document in the Security Management Plan how the Supplier and its Sub-contractors will:
- (a) comply with the requirements set out in this Security Schedule and the Contract in order to ensure the security of the Buyer Data and the Supplier Information Management System; and
 - (b) ensure that the operation of the Supplier Information Management System and the provision of the Services does not give rise to any information security risks greater than those set out in that Statement of Information Risk Appetite (where one has been provided).
- 13.3 The Supplier must ensure that:
- (a) the Security Management Plan accurately represents the Supplier Information Management System;
 - (b) the Supplier Information Management System will meet the requirements of this Security Schedule and the Statement of Risk Appetite (where one has been provided); and
 - (c) the residual risks of the Supplier Information Management System are no greater than those provided for in the Statement of Risk Appetite (where one has been provided).

Preparation of Security Management Plan

- 13.4 The Supplier must prepare and submit the Security Management Plan to the Buyer:
- (a) within 20 Working Days of contract agreement; or
 - (b) by the date specified in the Detailed Implementation Plan; or
 - (c) if no such date is specified, in sufficient time to allow for the Buyer to review and approve the Security Management Plan before the first Operational Service Commencement Date.
- 13.5 If Paragraph 13.4(b) applies, and any delay resulting from the Buyer's review and approval of the Security Management Plan causes or contributes to Supplier Non-Performance under Clause 32.1, that delay is not a Buyer Cause and the Supplier shall not be entitled to any relief or compensation under Clause 32.

Contents of Security Management Plan

- 13.6 The Security Management Plan must use the template in Appendix 5 and must include:
- (a) a formal risk assessment of, and a risk treatment plan for, the Supplier Information Management System;

- (b) a completed ISO/IEC 27001:2022 statement of applicability for the Supplier Information Management System;
- (c) the process for managing any security risks from Sub-contractors and third parties with access to the Services, the Supplier Information Management System or the Buyer Data;
- (d) unless such requirement is waived by the Buyer, the controls the Supplier will implement in respect of the Services and all processes associated with the delivery of the Services, including:
 - (i) the Buyer Premises;
 - (ii) the Sites;
 - (iii) the Supplier System;
 - (iv) the Buyer System (to the extent that it is under the control of the Supplier); and
 - (v) any IT, Information and data (including the Confidential Information of the Buyer and the Buyer Data) to the extent used by the Buyer or the Supplier:
 - (A) in connection with this Contract or
 - (B) in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;
- (e) evidence that the Supplier and each applicable Sub-contractor is compliant with the Certification Requirements; and
- (f) the diagram documenting the Supplier Information Management System, the Wider Information Management System and the boundary between them (created under Paragraph 11).
- (g) an assessment of the Supplier Information Management System against the requirements of this Security Schedule , including the Security Requirements and the Security Requirements for Development (where applicable);
- (h) the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Buyer Data, the Buyer, the Services and/or users of the Services; and
- (i) the following information, so far as is applicable, in respect of each Sub-contractor:
 - (i) the Sub-contractor's:
 - (A) legal name;
 - (B) trading name (if any); and
 - (C) registration details (where the Sub-contractor is not an individual);
 - (ii) the Relevant Certifications held by the Sub-contractor;
 - (iii) the Sites used by the Sub-contractor;

- (iv) the Services provided, or contributed to, by the Sub-contractor;
 - (v) the access the Sub-contractor has to the Supplier Information Management System;
 - (vi) the Buyer Data Processed by the Sub-contractor;
 - (vii) the Processing that the Sub-contractor will undertake in respect of the Buyer Data; and
 - (viii) the measures the Sub-contractor has in place to comply with the requirements of this Security Schedule);
- (j) the Register of Support Locations and Third Party Tools;
 - (k) the Modules Register;
 - (l) the Support Register; and
 - (m) details of the protective monitoring that the Supplier will undertake in accordance with paragraph 12 of the Security Requirements, including:
 - (i) the additional audit and monitoring the Supplier will undertake of the Supplier Information Management System; and
 - (ii) the retention periods for audit records and event logs.

14 Monitoring and updating Security Management Plan

Updating Security Management Plan

- 14.1 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.

Monitoring

- 14.2 The Supplier, where it plans to undertake, or after becoming aware of, any of the following:
- (a) a significant change to the components or architecture of the Supplier Information Management System;
 - (b) a significant change in the boundary between the Supplier Information Management System and the Wider Information Management System;
 - (c) a significant change in the operation of the Supplier Information Management System;
 - (d) the replacement of an existing, or the appointment of a new:
 - (i) SIMS Sub-contractor; or
 - (ii) Sub-contractor that Processes Buyer Data;
 - (e) a significant change in the quantity of Personal Data held within the Service; and/or

- (f) where the Supplier has previously Processed Buyer Data that is Personal Data, not including Special Category Personal Data, it proposes to start to Process Buyer Data that is Special Category Personal Data under this Contract;
must:
 - (g) within 2 Working Days notify the Buyer; and
 - (h) within 10 Working Days, or such other timescale as may be agreed with the Buyer, update the Security Management Plan and provide the Buyer with a copy that document for review and approval.
- 14.3 Paragraph 14.2 applies in addition to, and not in substitution of, the Parties' obligations to comply with the Change Control Procedure for any Contract Change or Operational Change.
- 14.4 Any proposed change under Paragraph 14.2(a), 14.2(b) or 14.2(f) is a Contract Change to which the Change Control Procedure applies.

15 Review and approval of Security Management Plan

- 15.1 Where the Supplier has prepared or updated the Security Management Plan the Buyer may review the plan and to do so may request such further information as the Buyer considers necessary or desirable.
- 15.2 At the conclusion of that review, it may issue to the Supplier:
- (c) where satisfied that the:
 - (i) identified risks to the Supplier Information Management System are adequately and appropriately addressed; and
 - (ii) that the residual risks are:
 - (A) either:
 - (1) where the Buyer has provided a Statement of Information Risk Appetite, reduced to the level anticipated by that statement; or
 - (2) where the Buyer has not provided a Statement of Information Risk Appetite, reduced to an acceptable level;
 - (B) understood and accepted by the Buyer; and
 - (C) recorded in the Residual Risk Statement;
- a Risk Management Approval Statement; or
- (d) where the Buyer considers that:
 - (i) the identified risks to the Supplier Information Management System have not been adequately or appropriately addressed; or
 - (ii) the residual risks to the Supplier Information Management System have not been reduced:

- (A) where the Buyer has Provided a Statement of Information Risk Appetite, to the level anticipated by that statement; or
- (B) where the Buyer has not Provided a Statement of Information Risk Appetite, to an acceptable level,

a Risk Management Rejection Notice, with the reasons for its decision.

16 Changes to the Supplier Information Management System

16.1 Notwithstanding anything in this Contract, the Supplier must obtain the approval of the Buyer before making any of the following changes to the Supplier Information Management System:

- (a) a significant change in the systems or components making up the Supplier Information Management System;
- (b) a significant change in the operation or management of the Supplier Information Management System; or
- (c) the appointment of a new, or the replacement of an existing:
 - (i) SIMS Sub-contractor; or
 - (ii) Sub-contractor that Processes Buyer Data.

16.2 In seeking the Buyer's approval to a proposed changes to the Supplier Information Management System, the Supplier must:

- (a) prepare a proposal for the Buyer setting out:
 - (i) details of the proposed changes to the Supplier Information Management System;
 - (ii) an assessment of the security implications of the proposed change;
 - (iii) a risk assessment of the proposed change;
- (b) provide that paper to the Buyer no later than 30 Working Days before the date on which the Supplier proposes to implement those changes.

16.3 The Buyer:

- (a) may request such further information as the Buyer considers necessary or desirable;
- (b) must provide its decision within 20 Working Days of the later of:
 - (i) the date on which it receives the proposal; or
 - (ii) the date on which it receives any requested further information;
- (c) must not:
 - (i) unreasonably refuse any proposal by the Supplier; and
 - (ii) must not make any approval subject to unreasonable conditions.

- 16.4 If the Buyer does not provide a decision within the period specified in Paragraph 16.3(b), the proposal shall be deemed to have been accepted.

Implementation of changes

- 16.5 Where the Supplier implements a necessary change to the Supplier Information Management System to address a security related risk or vulnerability, the Supplier shall effect such change at its own cost and expense.
- 16.6 If the Supplier does not implement a necessary change to the Supplier Information Management System to address a security related risk or vulnerability:
- (a) that failure is a material Default; and
 - (b) the Supplier shall:
 - (i) immediately cease using the Supplier Information Management System to Process Buyer Data either:
 - (A) until the Default is remedied, or
 - (B) unless directed otherwise by the Buyer in writing and then only in accordance with the Buyer's written directions; and
 - (ii) where such material Default is capable of remedy, remedy such material Default within the timescales set by the Buyer (considering the security risks the material Default presents to the Services and/or the Supplier Information Management System).

17 Remediation Action Plan

Preparation of Remediation Action Plan

- 17.1 Where:
- (a) the Buyer issues a Risk Management Rejection Notice; or
 - (b) the Supplier receives a Security Test report identifies vulnerabilities in, or makes findings in respect of, the Supplier Information Management System,
- the Supplier must within 20 Working Days of receiving the notice or report, as applicable, prepare a plan addressing the matters raised in the notice or report, as applicable (a "**Remediation Action Plan**").
- 17.2 The Remediation Action Plan must, in respect of each matter raised by Risk Management Rejection notice or the Security Test report:
- (a) how the matter will be remedied;
 - (b) the date by which the matter will be remedied; and
 - (c) the tests that the Supplier proposes to perform to confirm that the matter has been remedied.

Consideration of Remediation Action Plan

17.3 The Supplier must

- (a) provide the Buyer with a copy of any Remediation Action Plan it prepares; and
- (b) have regarded to any comments the Buyer provides in the Remediation Action Plan.

Implementing an approved Remediation Action Plan

17.4 In implementing the Remediation Action Plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.

17.5 If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within 2 Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:

- (a) provide the Buyer with a full, unedited and unredacted copy of the test report;
- (b) implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;
- (c) as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

18 Independent Security Adviser

18.1 The Buyer may require the appointment of an Independent Security Adviser where:

- (a) there is a proposed change to the Supplier Information Management System (see Paragraph 11.5);
- (b) the Buyer issues two or more Risk Management Rejection Notices (see Paragraph 15.2(b)); or
- (a) a Security Test (see paragraph 10 of the Security Requirements) report identifies more than 10 vulnerabilities classified as either critical or high; or

18.2 Where the Buyer requires the appointment of an Independent Security Adviser the Independent Security Adviser shall be:

- (b) a person selected by the Supplier and approved by the Buyer; or
- (c) where
 - (i) the Buyer does not approve the persons selected by the Supplier; or
 - (ii) the Supplier does not select any person within 10 Working Days of the date of the notice requiring the Independent Security Adviser's appointment,

a person selected by the Buyer.

18.3 The terms of the Independent Security Adviser's appointment shall require that person to:

- (d) undertake a detailed review, including a full root cause analysis where the Independent Security Adviser considers it appropriate to do so, of the circumstances that led to that person's appointment; and
- (e) provide advice and recommendations on:
 - (i) steps the Supplier can reasonably take to improve the security of the Supplier Information Management System; and
 - (ii) where relevant, how the Supplier may mitigate the effects of, and remedy, those and to avoid the occurrence of similar circumstances to those leading to the appointment of the Independent Security Adviser in the future.

18.4 The Supplier must permit, and must ensure that relevant Sub-contractors permit, the Independent Security Adviser to:

- (f) observe the conduct of and work alongside the Supplier Personnel to the extent that the Independent Security Adviser considers reasonable and proportionate having regard to reason for their appointment;
- (g) gather any information the Independent Security Adviser considers relevant in the furtherance of their appointment;
- (h) write reports and provide information to the Buyer in connection with the steps being taken by the Supplier to remedy the matters leading to the Independent Security Adviser's appointment;
- (i) make recommendations to the Buyer and/or the Supplier as to how the matters leading to their appointment might be mitigated or avoided in the future; and/or
- (j) take any other steps that the Buyer and/or the Independent Security Adviser reasonably considers necessary or expedient in order to mitigate or rectify matters leading to the Independent Security Adviser's appointment.

18.5 The Supplier must, and ensure that relevant Sub-contractors:

- (k) where relevant, work alongside, provide information to, co-operate in good faith with and adopt any reasonable methodology in providing the Services recommended by the Independent Security Adviser in order to mitigate or rectify any of the vulnerabilities that led to the appointment of the Independent Security Adviser;
- (l) ensure that the Independent Security Adviser has all the access it may require in order to carry out its objective, including access to the Assets;
- (m) submit to such monitoring as the Buyer and/or the Independent Security Adviser considers reasonable and proportionate in respect of the matters giving rise to their appointment;
- (n) implement any recommendations (including additional security measures and/or controls) made by the Independent Security Adviser that have been approved by the Buyer within the timescales given by the Independent Security Adviser; and
- (o) not terminate the appointment of the Independent Security Adviser without the prior consent of the Buyer (unless such consent has been unreasonably withheld).

18.6 The Supplier shall be responsible for:

- (p) the costs of appointing, and the fees charged by, the Independent Security Adviser; and
- (q) its own costs in connection with any action required by the Buyer and/or the Independent Security Adviser.

If the Supplier or any relevant Sub-contractor:

- (r) fails to perform any of the steps required by the Buyer in the notice appointing the Independent Security Adviser; and/or
- (s) is in Default of any of its obligations under this Paragraph 18,

this is a material Default that is capable of remedy.

19 Withholding of Charges

19.1 The Buyer may withhold some or all of the Charges in accordance with the provisions of this Paragraph 19 where:

- (t) the Supplier is in material Default of any of its obligations under this Security Schedule ; or
- (u) any of the following matters occurs (where those matters arise from a Default by the Supplier of its obligations under this Security Schedule):
 - (i) the Buyer is entitled to terminate the Contract for material Default on any of the grounds set out in Clause 35.2.1 (a) to (e) inclusive; or
 - (ii) the Supplier commits a material Default that is capable of remedy and the Buyer is entitled to step-in pursuant to Clause 31.13(b) or (c).

19.2 The Buyer may withhold an amount of the Charges that it considers sufficient, in its sole discretion, to incentivise the Supplier to perform the obligations it has Defaulted upon.

Before withholding any Charges under Paragraph 19.1 the Buyer must

- (v) provide written notice to the Supplier setting out:
 - (i) the Default in respect of which the Buyer has decided to withhold some or all of the Charges;
 - (ii) the amount of the Charges that the Buyer will withhold;
 - (iii) the steps the Supplier must take to remedy the Default;
 - (iv) the date by which the Supplier must remedy the Default;
 - (v) the invoice in respect of which the Buyer will withhold the Charges; and
- (w) consider any representations that the Supplier may make concerning the Buyer's decision.

19.3 Where the Supplier does not remedy the Default by the date specified in the notice given under Paragraph 19.3(a), the Buyer may retain the withheld amount.

The Supplier acknowledges:

- (x) the legitimate interest that the Buyer has in ensuring the security of the Supplier Information Management System and the Buyer Data and, as a consequence, the performance by the Supplier of its obligations under this Security Schedule ; and
- (y) that any Charges that are retained by the Buyer are not out of all proportion to the Buyer's legitimate interest, even where:
 - (i) the Buyer has not suffered any Losses as a result of the Supplier's Default; or
 - (ii) the value of the Losses suffered by the Buyer as a result of the Supplier's Default is lower than the amount of the Charges retained

19.4 The Buyer's right to withhold or retain any amount under this Paragraph 19 are in addition to any other rights that the Buyer may have under this Contract or in Law, including any right to claim damages for Losses it suffers arising from the Default.

20 Access to Buyer System

Where the Supplier, a Sub-contractor or any of the Supplier Personnel is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Sub-contractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

1. Location

Location for Relevant Activities

- 1.1 Unless otherwise agreed with the Buyer, the Supplier must, and ensure that its Sub-contractors, at all times:
- (z) store, access or process Buyer Data;
 - (aa) undertake the Development Activity; and
 - (bb) host the Development Environment,
- (together, the “**Relevant Activities**”)
- only in or from the geographic areas permitted by the Buyer in Paragraph 1.
- 1.2 Where the Buyer has permitted the Supplier and its Sub-contractors to perform the Relevant Activities outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors undertake the Relevant Activities in a facility operated by an entity where:
- (a) the entity has entered into a binding Contract with the Supplier or Sub-contractor (as applicable);
 - (b) that binding Contract includes obligations on the entity in relation to security management equivalent to those imposed on Sub-contractors in this Security Schedule ;
 - (c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding Contract;
 - (d) the Supplier has provided the Buyer with such information as the Buyer requires concerning:
 - (i) the entity;
 - (ii) the arrangements with the entity; and
 - (iii) the entity's compliance with the binding Contract; and
 - (e) the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.8.
- 1.3 Where the Supplier cannot comply with one or more of the requirements of paragraph 1.2:
- (a) it must provide the Buyer with such information as the Buyer requests concerning:
 - (i) the security controls in places at the relevant location or locations; and
 - (ii) where certain security controls are not, or only partially, implemented the reasons for this;

- (b) the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and
- (c) if the Buyer does not grant permission to use that location or those locations, the Supplier must, within such period as the Buyer may specify:
 - (i) cease to store, access or process Buyer Data at that location or those locations;
 - (ii) sanitise, in accordance with instructions from the Buyer, such equipment within the information and communications technology system used to store, access or process Buyer Data at that location, or those locations, as the Buyer may specify.

Support Locations

- 1.4 The Supplier must ensure that all Support Locations are located only in the geographic areas permitted by the Buyer.
- 1.5 Where the Buyer has permitted the Supplier and its Sub-contractors to operate Support Locations outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors operate the Support Locations in a facility operated by an entity where
 - (a) the entity has entered into a binding Contract with the Supplier or Sub-contractor (as applicable);
 - (b) the binding Contract includes obligations in relations to security management at least as onerous as those imposed on any Sub-contractor by this Security Schedule ;
 - (c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding Contract;
 - (d) the Supplier has provided the Buyer with such information as the Buyer requires concerning:
 - (i) the entity;
 - (ii) the arrangements with the entity; and
 - (iii) the entity's compliance with the binding Contract; and
 - (iv) the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.8.

Third-party Tools

- 1.6 The Supplier must use, and ensure that Sub-contractors use, only those Third-party Tools included in the Register of Support Locations and Third-party Tools.
- 1.7 The Supplier must not, and must not allow Sub-contractors to, use:
 - 1.7.1 a Third-party Tool other than for the activity specified for that Third-party Tool in the Register of Support Locations and Third-party Tools; or
 - 1.7.2 a new Third-party Tool, or replace an existing Third-party Tool, without the permission of the Buyer.

Prohibited Activities

- 1.8 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken some or all of the Relevant Activities or operate Support Locations (a “**Prohibited Activity**”).
- 1.8.1 in any particular country or group of countries;
- 1.8.2 in or using facilities operated by any particular entity or group of entities; or
- 1.8.3 in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity,
- (a “**Prohibition Notice**”).
- 1.9 Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant Activities or operates any Support Locations affected by the notice, the Supplier must, and must procure that Sub-contractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.
- 1.10 Nothing in this Paragraph 1 shall affect the Parties obligations to comply with Clause 34.7.4 and the conditions set out therein shall continue to apply in addition to the requirements of this Paragraph 1.

2. Vetting, Training and Staff Access

Vetting before performing or managing Services

- 2.1 The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel in:
- 2.1.1 Development Activity;
- 2.1.2 any activity that provides access to the Development Environment; or
- 2.1.3 any activity relating to the performance and management of the Services
- unless:
- 2.1.4 that individual has passed the security checks listed in paragraph 2.2; or
- 2.1.5 the Buyer has given prior written permission for a named individual to perform a specific role.
- 2.2 For the purposes of paragraph 2.1, the security checks are:
- 2.2.1 The checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:
- 2.2.1.1 the individual's identity;
- 2.2.1.2 where that individual will work in the United Kingdom, the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;
- 2.2.1.3 the individual's previous employment history; and

2.2.1.4 that the individual has no Relevant Convictions;

2.2.2 national security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or

2.2.3 such other checks for the Supplier Personnel of Sub-contractors as the Buyer may specify.

Annual training

2.3 The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:

2.3.1 General training concerning security and data handling; and

2.3.2 Phishing, including the dangers from ransomware and other malware.

Staff access

2.4 The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.

2.5 The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.

2.6 Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel's access to the Buyer Data, or part of that Buyer Data specified by the Buyer, as soon as practicable and in any event within 24 hours of the request.

Exception for certain Sub-contractors

2.7 Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:

2.7.1 as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;

2.7.2 provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor Personnel will perform as the Buyer reasonably requires; and

2.7.3 comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.

3. End-user Devices

3.1 The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data or Code is stored or processed in accordance the following requirements:

- 3.1.1 the operating system and any applications that store, process or have access to Buyer Data or Code must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
- 3.1.2 users must authenticate before gaining access;
- 3.1.3 all Buyer Data and Code must be encrypted using a encryption tool agreed to by the Buyer;
- 3.1.4 the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
- 3.1.5 the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Buyer Data and Code to ensure the security of that Buyer Data and Code;
- 3.1.6 the Supplier or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data or Code stored on the device and prevent any user or group of users from accessing the device;
- 3.1.7 all End-user Devices are within the scope of any Relevant Certification.
- 3.2 The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Contract.
- 3.3 Where there any conflict between the requirements of this Security Schedule and the requirements of the NCSC Device Guidance, the requirements of this Schedule take precedence.

4. Hardware and software support

- 4.1 The Supplier must ensure that all software used to provide the Services remains at all times in full security support, including any extended or bespoke security support.
- 4.2 The Supplier must produce and maintain a register of all software that form the Supplier Information Management System (the “**Support Register**”).
- 4.3 The Support Register must include in respect of each item of software:
 - 4.3.1 the date, so far as it is known, that the item will cease to be in mainstream security support; and
 - 4.3.2 the Supplier’s plans to upgrade the item before it ceases to be in mainstream security support.
- 4.4 The Supplier must:
 - 4.4.1 review and update the Support Register:
 - 4.4.1.1 within 10 Working Days of becoming aware of the date on which, or any change to the date on which, any item of software will cease to be in mainstream security support;

- 4.4.1.2 within 10 Working Days of introducing new software, or removing existing software, from the Supplier Information Management System; and
 - 4.4.1.3 at least once every 12 months;
 - 4.4.2 provide the Buyer with a copy of the Support Register:
 - 4.4.2.1 whenever it updates the Support Register; and
 - 4.4.2.2 otherwise when the Buyer requests.
- 4.5 Where any element of the Developed System consists of COTS Software, the Supplier shall ensure:
 - 4.5.1 those elements are always in mainstream or extended security support from the relevant vendor; and
 - 4.5.2 the COTS Software is not more than one version or major release behind the latest version of the software.
- 4.6 The Supplier shall ensure that all hardware used to provide the Services, whether used by the Supplier or any Sub-contractor is, at all times, remains in mainstream vendor support, that is, that in respect of the hardware, the vendor continues to provide:
 - 4.6.1 regular firmware updates to the hardware; and
 - 4.6.2 a physical repair or replacement service for the hardware.

5. Encryption

- 5.1 Before Processing any Buyer Data, the Supplier must agree with the Buyer the encryption methods that it and any Sub-contractors that Process Buyer Data will use to comply with this paragraph 5.
- 5.2 Where this paragraph 5 requires Buyer Data to be encrypted, the Supplier must use, and ensure that Subcontractors use, the methods agreed by the Buyer under paragraph 5.1.
- 5.3 Notwithstanding anything in the specification for the Developed System or this Contract, the Supplier must ensure that the Developed System encrypts Buyer Data:
 - 5.3.1 when the Buyer Data is stored at any time when no operation is being performed on it; and
 - 5.3.2 when the Buyer Data is transmitted.
- 5.4 Unless paragraph 5.5 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer Data is encrypted:
 - 5.4.1 when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and
 - 5.4.2 when transmitted.
- 5.5 Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 5.4, the Supplier must:

- 5.5.1 immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
 - 5.5.2 provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;
 - 5.5.3 provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.
- 5.6 The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.
- 5.7 Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
- 5.7.1 the subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;
 - 5.7.2 the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Buyer Data.
- 5.8 Where the Buyer and Supplier do not reach Contract within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Buyer Data, either party may refer the matter to be determined by an expert in accordance with the Dispute Resolution Procedure.

6. Email

- 6.1 Notwithstanding anything in the specification for the Developed System or this Contract, the Supplier must ensure that where the Developed System will provide an Email Service to the Buyer, the Developed System:
- 6.1.1 supports transport layer security ("**TLS**") version 1.2, or higher, for sending and receiving emails;
 - 6.1.2 supports TLS Reporting ("**TLS-RPT**");
 - 6.1.3 is capable of implementing:
 - 6.1.3.1 domain-based message authentication, reporting and conformance ("**DMARC**");
 - 6.1.3.2 sender policy framework ("**SPF**"); and
 - 6.1.3.3 domain keys identified mail ("**DKIM**"); and
 - 6.1.4 is capable of complying in all respects with any guidance concerning email security as issued or updated from time to time by:
 - 6.1.4.1 the UK Government (current version at <https://www.gov.uk/guidance/set-up-government-email-services-securely>); or

7. DNS

Unless otherwise agreed by the Buyer, the Supplier must ensure that the Developed System uses the UK public sector Protective DNS (“**PDNS**”) service to resolve internet DNS queries.

8. Malicious Software

- 8.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.
- 8.2 The Supplier must ensure that such Anti-virus Software:
 - 8.2.1 prevents the installation of the most common forms of Malicious Software in the Supplier Information Management System and the Development Environment;
 - 8.2.2 is configured to perform automatic software and definition updates;
 - 8.2.3 provides for all updates to be the Anti-virus Software to be deployed within 10 Working Days of the update’s release by the vendor;
 - 8.2.4 performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and
 - 8.2.5 where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.
- 8.3 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Buyer Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.
- 8.4 The Supplier must at all times, during and after the Term, on written demand indemnify the Buyer and keep the Buyer indemnified, against all Losses incurred by, awarded against or agreed to be paid by the Buyer arising from any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Supplier, or a Sub-contractor, to comply with this paragraph .

9. Vulnerabilities

- 9.1 Unless the Buyer otherwise agrees, the Supplier must ensure that it or any relevant Sub-contractor applies security patches to any vulnerabilities in the Supplier Information Management System no later than:
 - 9.1.1 7 days after the public release of patches for vulnerabilities classified as “critical”;
 - 9.1.2 30 days after the public release of patches for vulnerabilities classified as “important”; and
 - 9.1.3 60 days after the public release of patches for vulnerabilities classified as “other”.

- 9.2 The Supplier must:
- 9.2.1 scan the Supplier Information Management System and the Development Environment at least once every month to identify any unpatched vulnerabilities; and
 - 9.2.2 if the scan identifies any unpatched vulnerabilities ensure they are patched in accordance with paragraph 9.1.
- 9.3 For the purposes of this paragraph 9, the Supplier must implement a method for classifying vulnerabilities to the Supplier Information Management System as “critical”, “important” or “other” that is aligned to recognised vulnerability assessment systems, such as:
- 9.3.1.1 the National Vulnerability Database’s vulnerability security ratings; or
 - 9.3.1.2 Microsoft’s security bulletin severity rating system.

10. Security testing

Responsibility for security testing

- 10.1 The Supplier is solely responsible for:
- (a) the costs of conducting any security testing required by this paragraph 10 (unless the Buyer gives notice under paragraph 10.2); and
 - (b) the costs of implementing any findings, or remedying any vulnerabilities, identified in that security testing.

Security tests by Buyer

- 10.2 The Buyer may, where it has significant concerns relating to the security of the Supplier Information Management System, give notice to the Supplier that the Buyer will undertake the Supplier Security Tests.
- 10.3 Where the Buyer gives notice under paragraph 10.2:
- (a) the Supplier shall provide such reasonable co-operation as the Buyer requests, including:
 - (i) such access to the Supplier Information Management System as the Buyer may request; and
 - (ii) such technical and other information relating to the Information Management System as the Buyer requests;
 - (b) the Buyer must provide a full, unedited and unredacted copy of the report relating to the IT Health Check as soon as reasonably practicable after the Buyer receives a copy of the report; and
 - (c) for the purposes of paragraphs 10.18 to 10.27:
 - (i) the Supplier must treat any IT Health Check commissioned by the Buyer as if it were such a report commissioned by the Supplier; and

- (ii) the time limits in paragraphs 10.18 and 10.20 run from the date on which the Buyer provides the Supplier with the copy of the report under paragraph (b).
- 10.4 In addition to its rights under paragraph 10.2, the Buyer and/or its authorised representatives may, at any time and without giving notice to the Supplier, carry out such tests (including penetration tests) as it may deem necessary in relation to:
 - (a) the Service;
 - (b) the Supplier Information Management System; and/or
 - (c) the Supplier's compliance with the Security Management Plan,
("Buyer Security Tests").
- 10.5 The Buyer shall take reasonable steps to notify the Supplier prior to carrying out such Buyer Security Tests to the extent that it is reasonably practicable for it to do so taking into account the nature of the Buyer Security Tests.
- 10.6 The Buyer shall notify the Supplier of the results of such Buyer Security Tests after completion of each Buyer Security Test.
- 10.7 The Buyer shall design and implement the Buyer Security Tests to minimise their impact on the delivery of the Services.
- 10.8 If an Buyer Security Tests causes Supplier Non-Performance, the Buyer Security Tests shall be treated as an Buyer Cause, except where the root cause of the Supplier Non-Performance was a security-related weakness or vulnerability exposed by the Buyer Security Tests.

Security tests by Supplier

- 10.9 The Supplier must:
 - (a) before submitting the draft Security Management Plan to the Buyer for an Assurance Decision;
 - (b) at least once during each Contract Year; and
 - (c) when required to do so by the Buyer;

undertake the following activities:

 - (d) conduct security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment (an **"IT Health Check"**) in accordance with paragraphs 10.15 to 10.17; and
 - (e) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with paragraphs 10.18 to 10.27.
- 10.10 In addition to its obligations under paragraph 10.9, the Supplier must undertake any tests required by:
 - (a) any Remediation Action Plan;
 - (b) the ISO27001 Certification Requirements;
 - (c) the Security Management Plan; and

- (d) the Buyer, following a Breach of Security or a significant change, as assessed by the Buyer, to the components or architecture of the Supplier Information Management System,

(each a “**Supplier Security Test**”).

10.11 The Supplier must

- (a) design and implement the Supplier Security Tests so as to minimise the impact on the delivery of the Services;
- (b) agree the date, timing, content and conduct of such Supplier Security Tests in advance with the Buyer.

10.12 Where the Supplier fully complies with paragraph 10.11, if a Supplier Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be entitled to relief in respect of such Performance Failure for that Measurement Period.

10.13 The Buyer may send a representative to witness the conduct of the Supplier Security Tests.

10.14 The Supplier shall provide the Buyer with a full, unedited and unredacted copy of the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable, and in any case within 10 Working Days, after completion of each Supplier Security Test

IT Health Checks

10.15 In arranging an IT Health Check, the Supplier must:

- (c) use only a CHECK Service Provider to perform the IT Health Check;
- (d) design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier Information Management System and the delivery of the Services.
- (e) promptly provide the Buyer with such technical and other information relating to the Supplier Information Management System as the Buyer requests;
- (f) include within the scope of the IT Health Check such tests as the Buyer requires;
- (g) agree with the Buyer the scope, aim and timing of the IT Health Check.

10.16 The Supplier must commission the IT Health Check in accordance with the scope, aim and timing agreed by the Buyer.

10.17 Following completion of an IT Health Check, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the report relating to the IT Health Check without delay and in any event within 10 Working Days of its receipt by the Supplier.

Remedying vulnerabilities

10.18 In addition to complying with Paragraphs 10.20 to 10.27, the Supplier must remedy:

- (a) any vulnerabilities classified as critical in a Security Test report within 5 Working Days of becoming aware of the vulnerability and its classification;
- (b) any vulnerabilities classified as high in a Security Test report within 1 month of becoming aware of the vulnerability and its classification; and

- (c) any vulnerabilities classified as medium in a Security Test report within 3 months of becoming aware of the vulnerability and its classification.

10.19 The Supplier must notify the Buyer immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as critical, high or medium in a Security Test report within the time periods specified in Paragraph 10.18.

Responding to a Security Test report

10.20 Where the Security Test report identifies vulnerabilities in, or makes findings in respect of, the Supplier Information Management System, the Supplier must within 20 Working Days of receiving the Security Test report, prepare and submit for approval to the Buyer a draft plan addressing the vulnerabilities and findings (the “**Remediation Action Plan**”).

10.21 Where the Buyer has commissioned a root cause analysis under Paragraph 10.28, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.

10.22 The draft Remediation Action Plan must, in respect of each vulnerability identified or finding made by the Security Test report:

- (a) how the vulnerability or finding will be remedied;
- (b) the date by which the vulnerability or finding will be remedied; and
- (c) the tests that the Supplier proposes to perform to confirm that the vulnerability has been remedied or the finding addressed.

10.23 The Supplier shall promptly provide the Buyer with such technical and other information relating to the Supplier Information Management System, the IT Health Check report or the draft Remediation Action Plan as the Buyer requests.

10.24 The Buyer may:

- (a) reject the draft Remediation Action Plan where it considers that the draft Remediation Action Plan is inadequate, providing its reasons for doing so, in which case:
 - (i) the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Buyer’s reasons; and
 - (ii) paragraph 10.22 to 10.24 shall apply, with appropriate modifications, to the revised draft Remediation Action Plan;
- (b) accept the draft Remediation Action Plan, in which case the Supplier must immediately start work on implementing the Remediation Action Plan in accordance with Paragraph 10.26 and 10.27.

10.25 Where the Buyer unreasonably:

- (a) delays its approval; or
- (b) rejects,

the draft Remediation Action Plan, the Supplier will not be in breach of this Contract to the extent it demonstrates that any breach:

- (c) arose directly from the Buyer unreasonably withholding or delaying, as appropriate, its approval of the draft Remediation Action Plan; and

- (d) would not have occurred had:
 - (i) the Buyer given its approval, or given its approval in a timely manner, to the draft Remediation Action Plan; and
 - (ii) the Supplier had implemented the draft Remediation Action Plan in accordance with its terms.

Implementing an approved Remediation Action Plan

- 10.26 In implementing the Remediation Action Plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.
- 10.27 If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within [2] Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:
 - (a) provide the Buyer with a full, unedited and unredacted copy of the test report;
 - (b) implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;
 - (c) as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

Significant vulnerabilities

- 10.28 Where:
 - (cc) a Security Test report identifies more than 10 vulnerabilities classified as either critical or high; or
 - (dd) the Buyer rejected a revised draft Remediation Action Plan,
the Buyer may, at the Supplier's cost, either:
 - (ee) appoint an independent and appropriately qualified and experienced security architect and adviser to perform a root cause analysis of the identified vulnerabilities; or
 - (ff) give notice to the Supplier requiring the appointment as soon as reasonably practicable, and in any event within 10 Working Days, of an Independent Security Adviser.

11. Access Control

- 11.1 The Supplier must, and must ensure that all Sub-contractors:
 - (gg) identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
 - (hh) require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;

- (ii) allow access only to those parts of the Supplier Information Management System and Sites that those persons require;
 - (jj) maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.
- 11.2 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:
 - 11.2.1 are allocated to a single, individual user;
 - 11.2.2 are accessible only from dedicated End-user Devices;
 - 11.2.3 are configured so that those accounts can only be used for system administration tasks;
 - 11.2.4 require passwords with high complexity that are changed regularly;
 - 11.2.5 automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive; and
 - 11.2.6 are:
 - 11.2.6.1** restricted to a single role or small number of roles;
 - 11.2.6.2** time limited; and
 - 11.2.6.3** restrict the Privileged User's access to the internet.
- 11.3 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that it logs all activity of the Privileged Users while those users access those accounts and keeps the activity logs for [20] Working Days before deletion.
- 11.4 The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different high-complexity passwords for their different accounts on the Supplier Information Management System.
- 11.5 The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in paragraphs 11.1 to 11.4.
- 11.6 The Supplier must, and must ensure that all Sub-contractors:
 - 11.6.1 configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and
 - 11.6.2 change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

12. Event logging and protective monitoring

Protective Monitoring System

12.1 The Supplier must, and must ensure that Sub-contractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code to:

- 12.1.1 identify and prevent potential Breaches of Security;
- 12.1.2 respond effectively and in a timely manner to Breaches of Security that do occur;
- 12.1.3 identify and implement changes to the Supplier Information Management System to prevent future Breaches of Security; and
- 12.1.4 help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier Information Management System or the Developed System

(the “**Protective Monitoring System**”).

12.2 The Protective Monitoring System must provide for:

- 12.2.1 event logs and audit records of access to the Supplier Information Management system; and
- 12.2.2 regular reports and alerts to identify:
 - 12.2.2.1** changing access trends;
 - 12.2.2.2** unusual usage patterns; or
 - 12.2.2.3** the access of greater than usual volumes of Buyer Data;
- 12.2.3** the detection and prevention of any attack on the Supplier Information Management System or the Development Environment using common cyber-attack techniques;
- 12.2.4 any other matters required by the Security Management Plan.

Event logs

12.3 The Supplier must ensure that, unless the Buyer otherwise agrees, any event logs do not log:

- 12.3.1 personal data, other than identifiers relating to users; or
- 12.3.2 sensitive data, such as credentials or security keys.

Provision of information to Buyer

12.4 The Supplier must provide the Buyer on request with:

- 12.4.1 full details of the Protective Monitoring System it has implemented; and
- 12.4.2 copies of monitoring logs and reports prepared as part of the Protective Monitoring System.

Changes to Protective Monitoring System

12.5 The Buyer may at any time require the Supplier to update the Protective Monitoring System to:

- 12.5.1 respond to a specific threat identified by the Buyer;
- 12.5.2 implement additional audit and monitoring requirements; and
- 12.5.3 stream any specified event logs to the Buyer's security information and event management system.

13. Audit rights

Right of audit

- 13.1 The Buyer may undertake an audit of the Supplier or any Sub-contractor to:
 - 13.1.1 verify the Supplier's or Sub-contractor's (as applicable) compliance with the requirements of this Security Schedule and the Data Protection Legislation as they apply to Buyer Data;
 - 13.1.2 inspect the Supplier Information Management System (or any part of it);
 - 13.1.3 review the integrity, confidentiality and security of the Buyer Data; and/or
 - 13.1.4 review the integrity and security of the Code.
- 13.2 Any audit undertaken under this Paragraph 13.1:
 - 13.2.1 may only take place during the Term and for a period of 18 months afterwards; and
 - 13.2.2 is in addition to and without prejudice to any other rights of audit the Buyer has under this Contract (including but not limited to, Clause 29).
- 13.3 The Buyer may not undertake more than one audit under Paragraph 13.1 in each calendar year unless the Buyer has reasonable grounds for believing:
 - 13.3.1 the Supplier or any Sub-contractor has not complied with its obligations under this Contract or the Data Protection Legislation as they apply to the Buyer Data;
 - 13.3.2 there has been or is likely to be a Breach of Security affecting the Buyer Data or the Code; or
 - 13.3.3 where vulnerabilities, or potential vulnerabilities, in the Code have been identified by:
 - 13.3.3.1** an IT Health Check; or
 - 13.3.3.2** a Breach of Security.

Conduct of audits

- 13.4 The Buyer must use reasonable endeavours to provide 30 Working Days' notice of an audit.
- 13.5 The Buyer must when conducting an audit:
 - 13.5.1 comply with all relevant policies and guidelines of the Supplier or Sub-contractor (as applicable) concerning access to the Supplier Information Management

System the Buyer considers reasonable having regard to the purpose of the audit; and

- 13.5.2 use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the Supplier or Sub-contractor (as applicable) or delay the provision of the Services.

- 13.6 The Supplier must, and must ensure that Sub-contractors, on demand provide the Buyer with all co-operation and assistance the Buyer may reasonably require, including:

- 13.6.1 all information requested by the Buyer within the scope of the audit;
- 13.6.2 access to the Supplier Information Management System; and
- 13.6.3 access to the Supplier Personnel.

Response to audit findings

- 13.7 Where an audit finds that:

- 13.7.1 the Supplier or a Sub-contractor has not complied with this Contract or the Data Protection Legislation as they apply to the Buyer Data; or
- 13.7.2 there has been or is likely to be a Breach of Security affecting the Buyer Data

the Buyer may require the Supplier to remedy those defaults at its own cost and expense and within the time reasonably specified by the Buyer.

- 13.8 The exercise by the Buyer of any rights it may have under this Paragraph 3 does not affect the exercise by it of any other or equivalent rights it may have under this Contract in respect of the audit findings.

14. Breach of Security

Reporting Breach of Security

- 14.1 If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours.

Immediate steps

- 14.2 The Supplier must, upon becoming aware of a Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other steps reasonably necessary to:
 - 14.2.1 minimise the extent of actual or potential harm caused by such Breach of Security;
 - 14.2.2 remedy such Breach of Security to the extent possible;
 - 14.2.3 apply a tested mitigation against any such Breach of Security; and
 - 14.2.4 prevent a further Breach of Security in the future which exploits the same root cause failure;

Subsequent action

- 14.3 As soon as reasonably practicable and, in any event, within 5 Working Days, or such other period agreed with the Buyer, following the Breach of Security, provide to the Buyer:
- 14.3.1 full details of the Breach of Security; and
 - 14.3.2 if required by the Buyer:
 - 14.3.2.1** a root cause analysis; and
 - 14.3.2.2** a draft plan addressing the root cause of the Breach of Security,
(the “**Breach Action Plan**”).
- 14.4 The draft Breach Action Plan must, in respect of each issue identified in the root cause analysis:
- 14.4.1 how the issue will be remedied;
 - 14.4.2 the date by which the issue will be remedied; and
 - 14.4.3 the tests that the Supplier proposes to perform to confirm that the issue has been remedied or the finding addressed.
- 14.5 The Supplier shall promptly provide the Buyer with such technical and other information relating to the draft Breach Action Plan as the Buyer requests.
- 14.6 The Buyer may:
- 14.6.1 reject the draft Breach Action Plan where it considers that the draft Breach Action Plan is inadequate, providing its reasons for doing so, in which case:
 - 14.6.1.1** the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Breach Action Plan submit a revised draft Breach Action Plan that takes into account the Buyer’s reasons; and
 - 14.6.1.2** paragraph 14.5 and 14.6 shall apply to the revised draft Breach Action Plan;
 - 14.6.2 accept the draft Breach Action Plan, in which case the Supplier must immediately start work on implementing the Breach Action Plan.

Assistance to Buyer

- 14.7 Where the Breach of Security concerns or is connected with the Buyer Data or the Code, the Supplier must provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer’s satisfaction.
- 14.8 The obligation to provide assistance under paragraph 14.8 continues notwithstanding the expiry or termination of this Contract.

Reporting of Breach of Security to regulator

- 14.9 Where the Law requires the Supplier report a Breach of Security to the appropriate regulator, the Supplier must:
- 14.9.1 make that report within the time limits:

- 14.9.1.1** specified by the relevant regulator; or
 - 14.9.1.2** otherwise required by Law;
 - 14.9.2 to the extent that the relevant regulator or the Law permits, provide the Buyer with a full, unredacted and unedited copy of that report at the same time it is sent to the relevant regulator.
- 14.10 Where the Law requires the Buyer to report a Breach of Security to the appropriate regulator, the Supplier must:
 - 14.10.1 provide such information and other input as the Buyer requires within the timescales specified by the Buyer;
 - 14.10.2 ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Buyer.
- 14.11 This Paragraph 14 applies in addition to, and not in substitution of, the Parties' obligations in respect of a Personal Data Breach set out in this Contract..

15. Return and Deletion of Buyer Data

- 15.1 The Supplier must create and maintain a register of
 - 15.1.1 all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer; and
 - 15.1.2 those parts of the Supplier Information Management System, including those parts of the Supplier Information Management System that are operated or controlled by any Sub-contractor, on which the Buyer Data is stored (the "**Buyer Data Register**").
- 15.2 The Supplier must:
 - 15.2.1 review and update the Buyer Data Register:
 - 15.2.1.1** within 10 Working Days of the Supplier or any Sub-contractor changes those parts of the Supplier Information Management System on which the Buyer Data is stored;
 - 15.2.1.2** within 10 Working Days of a significant change in the volume, nature or overall sensitivity of the Buyer Data stored on the Supplier Information Management System;
 - 15.2.1.3** at least once every 12 (twelve) months; and
 - 15.2.2 provide the Buyer with a copy of the Buyer Data Register:
 - 15.2.2.1 whenever it updates the Buyer Data Register; and
 - 15.2.2.2** otherwise when the Buyer requests.
- 15.3 The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code:
 - 15.3.1 when requested to do so by the Buyer; and

- 15.3.2 using a deletion method agreed with the Buyer that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.
- 15.4 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code:
 - 15.4.1 when requested to do so by the Buyer; and
 - 15.4.2 using the method specified by the Buyer.

1. Secure Software Development by Design

- 1.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, implement secure development and deployment practices to ensure that:
 - 1.1.1 no malicious code is introduced into the Developed System or the Supplier Information Management System.
 - 1.1.2 the Developed System can continue to function in accordance with the Specification:
 - 1.1.2.1** in unforeseen circumstances; and
 - 1.1.2.2** notwithstanding any attack on the Developed System using common cyber-attack techniques, including attacks using those vulnerabilities identified at any time in the OWASP Top Ten.
- 1.2 To those ends, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:
 - 1.2.1 comply with the Secure Development Guidance as if its requirements were terms of this Contract; and
 - 1.2.2 document the steps taken to comply with that guidance as part of the Security Management Plan.
- 1.3 In particular, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:
 - 1.3.1 ensure that all Supplier Personnel engaged in Development Activity are:
 - 1.3.1.1** trained and experienced in secure by design code development;
 - 1.3.1.2** provided with regular training in secure software development and deployment;
 - 1.3.2 ensure that all Code:
 - 1.3.2.1** is subject to a clear, well-organised, logical and documented architecture;
 - 1.3.2.2** follows OWASP Secure Coding Practice
 - 1.3.2.3** follows recognised secure coding standard, where one is available;
 - 1.3.2.4** employs consistent naming conventions;
 - 1.3.2.5** is coded in a consistent manner and style;
 - 1.3.2.6** is clearly and adequately documented to set out the function of each section of code;
 - 1.3.2.7** is subject to appropriate levels of review through automated and non-automated methods both as part of:

- (a) any original coding; and
 - (b) at any time the Code is changed;
- 1.3.3 ensure that all Development Environments:
 - 1.3.3.1 protect access credentials and secret keys;
 - 1.3.3.2 is logically separate from all other environments, including production systems, operated by the Supplier or Sub-contractor;
 - 1.3.3.3 requires multi-factor authentication to access;
 - 1.3.3.4 have onward technical controls to protect the Developed System or the Supplier Information Management System in the event a Development Environment is compromised;
 - 1.3.3.5 use network architecture controls to constrain access from the Development Environment to the Developed System or the Supplier Information Management System;

2. Secure Architecture

- 2.1 The Supplier shall design and build the Developed System in a manner consistent with:
 - 15.4.3 the NCSC's guidance on "Security Design Principles for Digital Services";
 - 15.4.4 where the Developed System will Process bulk data, the NCSC's guidance on "Bulk Data Principles"; and
 - 15.4.5 the NCSC's guidance on "Cloud Security Principles".
- 2.2 Where any of the documents referred to in paragraph 2.1 provides for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.

3. Code Repository and Deployment Pipeline

- 3.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity:
 - (kk) when using a cloud-based code depository for the deployment pipeline, use only a cloud-based code depository that has been assessed against the NCSC Cloud Security Principles;
 - (ll) ensure user access to code repositories is authenticated using credentials, with passwords or private keys;
 - (mm) ensure secret credentials are separated from source code.
 - (nn) run automatic security testing as part of any deployment of the Developed System.

4. Development and Testing Data

- 4.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, use only anonymised, dummy or synthetic data when using data within the Development Environment for the purposes of development and testing,

5. Code Reviews

- 5.1 The Supplier must:
- 5.1.1 regularly; or
 - 5.1.2 as required by the Buyer
- review the Code in accordance with the requirements of this paragraph 5 (a “**Code Review**”).
- 5.2 Before conducting any Code Review, the Supplier must agree with the Buyer:
- 5.2.1 the modules or elements of the Code subject to the Code Review;
 - 5.2.2 the development state at which the Code Review will take place;
 - 5.2.3 any specific security vulnerabilities the Code Review will assess; and
 - 5.2.4 the frequency of any Code Reviews (the “**Code Review Plan**”).
- 5.3 For the avoidance of doubt the Code Review Plan may specify different modules or elements of the Code are reviewed at a different development state, for different security vulnerabilities and at different frequencies.
- 5.4 The Supplier:
- 5.4.1 must undertake Code Reviews in accordance with the Code Review Plan; and
 - 5.4.2 may undertake Code Reviews by automated means if this is consistent with the approach specified in the Code review Plan.
- 5.5 No later than 10 Working Days or each Code Review, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the Code Review Report.
- 5.6 Where the Code Review identifies any security vulnerabilities, the Supplier must:
- 5.6.1 remedy these at its own cost and expense;
 - 5.6.2 ensure, so far as reasonably practicable, that the identified security vulnerabilities are not present in any other modules or code elements; and
 - 5.6.3 modify its approach to undertaking the Development Activities to ensure, so far as is practicable, the identified security vulnerabilities will not re-occur; and
 - 5.6.4 provide the Buyer with such information as it requests about the steps the Supplier takes under this paragraph 5.6.

6. Third-party Software

- 6.1 The Supplier must not, and must ensure that Sub-contractors do not, use any software to Process Buyer Data where the licence terms of that software purport to grant the licensor rights to Process the Buyer Data greater than those rights strictly necessary for the use of the software.

7. Third-party Software Modules

- 7.1 Where the Supplier or a Sub-contractor incorporates a Third-party Software Module into the Code, the Supplier must:
- 7.1.1 verify the source and integrity of the Third-party Software Module by cryptographic signing or such other measure that provides the same level of assurance;
 - 7.1.2 perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Software Module;
 - 7.1.3 continue to monitor any such Third-party Software Module so as to ensure it promptly becomes aware of any newly-discovered security vulnerabilities;
 - 7.1.4 take appropriate steps to minimise the effect of any such security vulnerability on the Developed System.
- 7.2 The Supplier must produce and maintain a register of all Third-party Software Modules that form part of the Code (the “**Modules Register**”).
- 7.3 The Modules Register must include, in respect of each Third-party Software Module:
- 7.3.1 full details of the developer of the module;
 - 7.3.2 the due diligence the Supplier undertook on the Third-party Software Module before deciding to use it;
 - 7.3.3 any recognised security vulnerabilities in the Third-party Software Module; and
 - 7.3.4 how the Supplier will minimise the effect of any such security vulnerability on the Developed System.
- 7.4 The Supplier must:
- 7.4.1 review and update the Modules Register:
 - 7.4.1.1 within 10 Working Days of becoming aware of a security vulnerability in any Third-party Software Module; and
 - 7.4.1.2 at least once every 6 (six) months;
 - 7.4.2 provide the Buyer with a copy of the Modules Register:
 - 7.4.2.1 whenever it updates the Modules Register; and
 - 7.4.2.2 otherwise when the Buyer requests.

Appendix 3 **Security Working Group**

1 Role of the Security Working Group

- 1.1 The Security Working Group shall be responsible for aspects set out in terms of Reference for the Security Working Group.
- 1.2 The Security Working Group:
 - (a) monitors and provides recommendations to the Supplier on the [Buyer-led Assurance] of the Supplier Information Management System;
 - (b) [See attachment for remainder of terms of reference for Security Working Group.

2 Meetings of the Security Working Group

- 2.1 Paragraphs 3.4 to 3.7 of Schedule 7 (Governance) shall apply to the Security Working Group as if it were a Board established under that Schedule.

3 Reports to the Security Working Group

- 3.1 The Supplier must provide the following reports no later than [five] Working Days before each meeting of the Security Working Group:
 - To be agreed as part of initial Security Working Group meeting.

4 Administration

- 4.1 [The Supplier is responsible for the secretarial functions of the SWG.]

Appendix 4 Sub-contractor Security Requirements and Security Requirements for Development

The table below sets out the Security Requirements and Development Requirements that do **not** apply to particular categories of Sub-contractors.

	SIMS Sub-contractors	Higher Risk Sub-contractors	Medium Risk Sub-contractors	Sub-contractors
Security Requirements that do not apply				
Development Requirements that do not apply				

