Crown Commercial Service

G-Cloud 12 Call-Off Contract

This Call-Off Contract for the G-Cloud 12 Framework Agreement (RM1557.12) includes:

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.

Digital Marketplace service ID number	48244 93812 09331
Call-Off Contract reference	Jaeger Ref. No. 24600
Call-Off Contract title	Secure Card Payment Service (SCPS)
Call-Off Contract description	A PCI Solution is to ensure that cardholder data is protected and secured when handled within DWP and to ensure compliance against PCI DSS and contribute to securing cardholder data for GDPR purposes.
Start date	16/03/2022
Expiry date	15/03/2024
Call-Off Contract value	**£3,320,434 excluding VAT**
Charging method	BACS
Purchase order number	To be provided following contract signature

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12).

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 Deliverables 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	Department for Work and Pensions (DWP) Caxton House Tothill Street London SW1H 9NA
To the Supplier	PCI-PAL (U.K.) Limited Unit 7 Gamma Terrace, West Road, Masterlord Estate Ipswich, Suffolk, IP3 9FF Company number: 03960535
Together the 'Parties'	

Principal contact details

For the Buyer:

[Redacted]

For the Supplier:

[Redacted]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 16/03/2022 and is valid for 24 months. The date and number of days or months is subject to clause 1.2 in Part B below.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least ninety (90) Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of thirty (30) days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-off Contract can be extended by the Buyer for two (2) period(s) of up to twelve (12) months each, by giving the Supplier three (3) months written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

Buyer contractual details

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

G-Cloud lot	This Call-Off Contract is for the provision of Services under: • Lot 2: Cloud software

G-Cloud services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:
	
	• A Secure Card Payment Service (SCPS) that utilises DTMF (Dual Tone Multi Frequency) masking technology to provide companies with a secure way of handling payments by phone without bringing their environments in scope of Payment Card Industry (PCI) Data Security Standard (DSS).
	
	  ○ [Redacted] licenses
	  ○ [Redacted] monthly minutes of inbound call charges
	  ○ [Redacted] monthly minutes of outbound call charges
	
	For the avoidance of doubt there is no minimum commitment to the volume of calls. Call charges will be billed as incurred.

Additional Services	In addition to the SCPS solution for inbound calls, the Supplier will continue to provide outbound PSTN connectivity to route calls into its outsourced contact centre environment until the end of August 2022 and thereafter on a month by month. • [Redacted] licenses • Continuation of current telephony service and billing arrangement Usage billed monthly. Outbound calls will be charged on a per second basis based on the pence per minute rates as detailed within the Rate Card shown in Schedule 2. Only calls to numbers beginning 09xx will be barred at the SCPS network level, calls to all other destinations will be allowed by the SCPS network and will be charged at the appropriate call rates. This includes calls to any premium number rate which will be fully charged to the DWP. Throughout the Term, the Supplier does not anticipate any minute price changes; however, in the event that third-party suppliers increase costs to the Supplier for the purchase of the minutes used with the Services, or revised Regulatory conditions are applied, the Supplier reserves the right to pass through such third-party supplier minute price increases to the Buyer upon no less than thirty (30) days prior written notice, which notice may be given in email form. In the event of any pass-through increase, Buyer costs will be only be agreed up to a capped limit of CPI % change as per the prevailing rate published by the National Audit Office.

Location	The Services will be delivered to: • Multiple Buyer locations in the UK as a cloud-based service.
Quality standards	The quality standards required for this Call-Off Contract are: • PCI DSS Level 1 Compliance
Technical standards:	The technical standards used as a requirement for this Call-Off Contract are: • PCI DSS Level 1 Compliance
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are detailed in the embedded document and summarised below: • SLA 1 – Payment Card Industry Voice Agents Availability • SLA 2 – Payment Card Industry Outbound Agents Availability • SLA 3 – Customer Interaction Service Availability • SLA 4 – Payment Card Industry Response Time • SLA 5 – Telephony Service Quality (MOS Score) • SLA 6 – Payment Card Industry Customer Payments The details of which can be found in Annex 1 of this Order Form titled "*PCI Telephony Solution Service Levels*". [Redacted] Service Credits Please refer to Annex 2 of this Order Form titled "*Service Credits*". Key Performance Indicators Please refer to Annex 3 of this Order Form titled "*Key Performance Indicators*". Service Boundaries This diagram illustrates the service boundaries and limits of responsibilities between the two parties: [Redacted]

Onboarding	The onboarding plan for this Call-Off Contract will: be agreed during the design phase of the project, including key milestones and associated tasks and risk register. The Supplier should employ a PRINCE2 tailored approach to project governance, ensuring appropriate project governance structures, processes and procedures are defined and agreed. This should include: • identifying, defining, and agreeing the project board and project management team structure, members, roles, and responsibilities, • developing effective communication, quality, and stakeholder management plans, • employing appropriate communication, change control and quality assurance methods and techniques, • agreeing the timing and frequency of communications which includes project meetings, checkpoint reports and general project status updates/reports, • agreeing project tolerances for time, cost quality and risk, • employing appropriate tools to track/manage project risks, actions, issues, and dependencies, • agreeing appropriate levels of project manager decision making authority and ensuring escalation of major issues and risks in a timely and appropriate manner. To the extent the Supplier is already engaged with the Buyer, the above activities shall constitute a review of the current approach.

Offboarding	The offboarding plan for this Call-Off Contract will: be agreed with the Buyer in-line with Call-Off Contract Terms and Conditions Section 21 and will address: • *Removing any data stores* (and, if required, transitioning to a Replacement Supplier) including, but not limited to, call data records (comprising phone number, non-obfuscated DTMF input (e.g. DTMF for IVR, but not for payment details) and date/timestamps) noting that Ofcom require Suppliers to hold caller data for seven (7) years, customer call agent details (such as user name, display name and credentials), customer identifiable service desk information, customer training and any other saved documentation. • *Disabling and disconnecting the SCPS application* • *Removing configurations and access to SCPS environments* including, but not limited to, deletion of customer routes/DDIs, SBC configurations (principally IP addresses), firewall rules and AWS MPLS peering • *Deleting credentials* within the Buyer's payment gateways Offboarding is included as part of the Call-off contract charges.
Collaboration agreement	Not applicable
Limit on Parties' liability	The annual total liability of either Party for all Property Defaults will not exceed **£1.73M**. The annual total liability for Buyer Data Defaults will not exceed **£1.73M** or **125%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability for all other Defaults will not exceed the greater of **£1.73M** or **125%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).

Insurance	The insurance(s) required will be: ● 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
Force majeure	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than sixty (60) consecutive days.
Audit	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits: • 7.4 to 7.12 (inclusive)
Buyer's responsibilities	The Buyer is responsible for: • Management of associated third parties (including, but not limited to, the rerouting of calls within the ICM platform at the request of the Supplier) during incidents • Provision and support of the physical links between the Supplier's data centres and the DWP's own data centres • Initial diagnostics of any service issues, including structured questioning as provided by the Supplier • Providing Peer level contacts within the DWP Helpdesk during incidents • Support Service for the Supplier regarding the DWP Place incident management system.

Buyer's equipment	The Buyer's equipment to be used with this Call-Off Contract includes: • Genesys Contact Centre • Siebel CRM application • Configuration of SBCs to provision a new route for Inbound and outbound calls for the Business Groups • Management of the ICM platform for the delivery of calls to the Supplier provided PSTN Numbers • Payment service providers, including Worldpay and GOV.UK Pay.

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners: The Supplier's core application is owned and managed by PCIPal; it is hosted in a Cloud Computing environment hosted by [Redacted] . The Supplier will be using a number of other partners to deliver the end to end service namely: [Redacted]

Call-Off Contract charges and payment

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

Payment method	The payment method for this Call-Off Contract is BACS.
Payment profile	The payment profile for this Call-Off Contract is: • Annual platform license fees payable in advance, and subsequent years can be paid quarterly in advance from the anniversary of the first years' licence • Any outbound call charges to be billed on a per second charging basis and are payable each calendar month in arrears.
Invoice details	The Supplier will issue electronic invoices in line with the Payment profile described above. The Buyer aims to pay within ten (10) days and commits to pay the Supplier within thirty (30) days of receipt of a valid invoice that is not disputed.
Who and where to send invoices to	Invoices must be sent to each of the following: 1. [Redacted] 2. Or by Post to: Department for Work and Pensions PO Box 406 SSCL Phoenix House, Celtic Springs Business Park Newport NP10 8FZ Buyer Billing Contacts: [Redacted]

Invoice information required	All invoices must include the: • Supplier's details • Purchase order number • Project Reference Number • A brief line description of charges linked to the PO • A date that the charges presented cover • A quantity and unit price Invoices to be raised upon completion of services delivered, unless otherwise agreed in the Payment profile.
Invoice frequency	Invoice will be sent to the Buyer in line with the schedule described in the above Payment profile.
Call-Off Contract value	The total value of this Call-Off Contract is: **£3,320,434 excluding VAT**
Call-Off Contract charges	The breakdown of the Charges is: [Redacted] In addition, any outbound call charges will be charged on a per second basis in line with the current rate card. For the avoidance of doubt there is no minimum commitment to volumes in relation to this Call-Off contract.

Additional Buyer terms

Performance of the Service and Deliverables	This Call-Off Contract will include the following milestones: • An Implementation Plan will be compiled for the Buyer's review in line with the stated Onboarding approach. • Exit and Off-boarding Plan
Guarantee	Not applicable
Warranties, representations	In addition to the incorporated Framework Agreement clause 4.1, the Supplier warrants and represents to the Buyer that: Not applicable
Supplemental requirements in addition to the Call-Off terms	Within the scope of the Call-Off Contract, the Supplier will: follow the DWP Policies and Procedures (PPs) listed below and shared between parties: • DWP AvM SD01 Outage Guidance v1.0 • Service Availability Reporting – PP Overview v1.0 • Change Management PP v2.0 Clean • SOCR Policy and Procedure v2.0 • Digital Service Management KPIs implementation • Problem Management Framework v3.0 Baselined • Event Management PP v1.0 • Knowledge Management Framework v2.2 Baselined • Major Incident PP v1.0 • Release and Deployment Management PP v1.0 • Request Fulfilment PP v1.0 clean • Service Catalogue Management v1.4 • Incident Priority Classification and Timescales • PCI Definition Document v01 Or any related or revised documents subsequently notified to the Supplier.

Alternative clauses	These Alternative Clauses, which have been selected from Schedule 4, will apply: Not applicable
Buyer specific amendments to/refinements of the Call-Off Contract terms	Within the scope of the Call-Off Contract: • With reference to Service level agreement above, if the Supplier consistently fails to achieve any individual Service Level for a period of three (3) consecutive months, the Buyer may exercise its right to terminate for breach and is entitled to recover any historic or future investment within the contracted year and subsequent term. <u>DWP Security</u> • DWP has legal and regulatory obligations to verify that the suppliers we work with have a reasonable standard of security in place to protect Buyer data and assets. DWP is committed to the protection of its information, assets and personnel and expects the same level of commitment from its suppliers (and sub-contractors if applicable). To protect the Department appropriately, DWP have recently reviewed its Security Supplier Assurance process and requirements and have made the applicable changes in line with industry good practice. These changes include but are not limited to: o Updated 'Security Schedule'. o Replacement of 'Security Management Plans' with the completion of the 'Information Security Questionnaire' as part of the tender submission. o Compliance with the DWP's relevant policies and standards, found at gov.uk. o Certification to industry good practice such as ISO27001 and Cyber Essentials Plus certification. • The Buyer security safeguards and requirements can be found in the DWP Enhanced Security Requirements at **Schedule 3** of this Order Form. The Schedule shall form part of this Call-Off Contract and shall take precedence in the event of any conflicts that may arise. • The Supplier is required to complete the Information Security Questionnaire (ISQ) to allows DWP to assess the supplier's compliance with DWP Security Schedule, Policy, Standard and industry good practice. The Supplier should complete this questionnaire, using the instructions tab, submitting evidence as

	necessary, including signing the declaration tab as part of your proposal to DWP. Protection on Information • The Supplier and any of its Sub-contractors, shall not access, process, host or transfer Buyer Data outside the United Kingdom without the prior written consent of the Buyer, and where the Buyer gives consent, the Supplier shall comply with any reasonable instructions notified to it by the Buyer in relation to the Buyer Data in question. The provisions set out in this paragraph shall apply to Landed Resources. • Where the Buyer has given its prior written consent to the Supplier to access, process, host, or transfer Buyer Data from premises outside the United Kingdom: a) the Supplier must notify the Buyer (in so far as they are not prohibited by Law) where any Regulatory Bodies seek to gain or has gained access to such Buyer Data. b) the Supplier shall take all necessary steps to prevent any access to, or disclosure of, any Buyer Data to any Regulatory Bodies outside the United Kingdom unless required by Law without any applicable exception or exemption. Historic Licenses In relation to any licenses procured from the Supplier by the Buyer, either historically or as part of this Call-Off Contract, these shall remain valid for continued use until the respective licences reach the anniversary date, providing that the Buyer has a valid contract which these can be transferred to.
Public Services Network (PSN)	The Public Services Network (PSN) is the government's secure network. If the G-Cloud Services are to be delivered over PSN this should be detailed here: Not applicable
Personal Data and Data Subjects	Annex 1 of Schedule 7 is applicable to this Call-Off Contract.

1. Formation of contract

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

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

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

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

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.

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

Signed	Supplier	Buyer
Name	[Redacted]	[Redacted]
Title	[Redacted]	[Redacted]
Signature	[Redacted]	[Redacted]
Date	02 March 2022	02 March 2022

Annex 1 – PCI Telephony Solution Service Levels

SLA 1– Payment Card Industry Voice Agents Availability	
Service Level Description	A measure of the percentage Inbound Voice Agent Availability of the Payment Card Industry Service.
Service Level Calculation	Availability shall be calculated as a percentage of the total time in a Calendar Month in accordance with the following formula: Service Availability = (MP – SD) / MP x 100% where: MP = Total time in minutes within the Calendar Month, excluding Planned Downtime, and SD = **the actual number of minutes for which the PCI Inbound Voice Service was unavailable during the Calendar,** to be calculated by $SD = \sum_{i=1}^{m} n_i t_i$ the formula: where: 1,2….m are the relevant Incidents during the Calendar Month. n_i is = 1 t_i is the number of minutes for which the PCI Service was Unavailable for the i'th Incident. Unavailable means that a Severity Level 1 or a Severity Level 2 Incident or a Severity Level 3 Incident has been raised against the PCI **Service.** NOTE: the calculated minutes would stop at the point where PCI Pal re-quested DWP to move inbound traffic to the alternate BT Route
Agreed Service Time	This Service shall be available 24 hours per day, 365 days per year (366 days in a leap year).
Agreed Service Measurement Time	This Service shall be measured 07:00 – 21:00 Monday – Friday (excluding Bank Holidays), 07:00 – 17:15 Saturdays, Sundays, and Bank Holidays.
Service Level	99.99%
Increased Impact Service Level	99.60%
Significant Failure Service Level	99.00%

SLA 2 – Payment Card Industry Outbound Agents Availability	
Service Level Description	A measure of the percentage Outbound Agent Availability of the Payment Card Industry Service.
Service Level Calculation	Availability shall be calculated as a percentage of the total time in a Calendar Month in accordance with the following formula: Service Availability = (MP – SD) / MP x 100% where: MP = Total time in minutes within the Calendar Month, excluding Planned Downtime, and SD = **the actual number of minutes for which the PCI Outbound Agent Service was unavailable during the Calendar,** to be calculated by $SD = \sum_{i=1}^{m} n_i t_i$ the formula: where: 1,2….m are the relevant Incidents during the Calendar Month. n_i is = 1 t_i is the number of minutes for which the PCI Service was Unavailable for the i'th Incident. Unavailable means that a Severity Level 1 or a Severity Level 2 Incident or a Severity Level 3 Incident has been raised against the PCI **Service.** NOTE: the calculated minutes would stop at the point where PCI Pal requested DWP to move outbound traffic to the alternate BT Route
Agreed Service Time	This Service shall be available 24 hours per day, 365 days per year (366 days in a leap year).
Agreed Service Measurement Time	This Service shall be measured 07:00 – 21:00 Monday – Friday (excluding Bank Holidays), 07:00 – 17:15 Saturdays, Sundays, and Bank Holidays.
Service Level	99.99%
Increased Impact Service Level	99.60%
Significant Failure Service Level	99.00%

SL3 – Customer Payment Service Availability	
Service Level Description	A measure of the percentage Availability of the Customer Payment Service.
Service Level Calculation	Availability shall be calculated as a percentage of the total agreed Service Measurement time (in minutes) in a Calendar Month that the Customer Interaction Service is able to process payments and onward route calls, in accordance with the following formula: Service Availability = **(B-A) x 100%** **B** Where: A is the total number of minutes that the Customer Payment Service is unavailable to process and onward route calls. B is the total agreed Service Measurement time (in minutes) in a Calendar Month. Unavailable means that a Severity Level 1 or a Severity Level 2 Incident or a Severity Level 3 Incident has been raised against the PCI payment Service**.**
Agreed Service Time	This Service shall be available 24 hours per day, 365 days per year (366 days in a leap year).
Agreed Service Measurement Time	This Service shall be measured 07:00 – 21:00 Monday – Friday (excluding Bank Holidays), 07:00 – 17:15 Saturdays, Sundays, and Bank Holidays.
Service Level	99.99%
Increased Impact Service Level	99.60%
Significant Failure Service Level	99.00%

SL4 – Payment Card Industry Response Time	
Service Level Description	A measure of the percentage of the Payment Card Industry Service instances going into Dual Tone Multi Frequency (DTMF) masking mode between the last PIN digit and confirmation message being sent to the Department within 1 second.
Service Level Calculation	Payment Card Industry Response Time shall be calculated as a percentage of the total number of Card Payments or Payment Resets initiated by Voice Agents or Outbound agents in a Calendar Month that the DTMF response time is within (3 seconds) in accordance with the following formula: Service Performance = $\frac{(B-A)}{B} \times 100\%$ Where: A is the total number of instances with a response time of 3 seconds or more during the Calendar Month. B is the total number of Payment/Reset instances initiated by Voice Agents or Outbound agents during the Calendar Month.
Agreed Service Time	This Service shall be available 24 hours per day, 365 days per year (366 days in a leap year).
Agreed Service Measurement Time	This Service shall be measured 07:00 – 21:00 Monday – Friday (excluding Bank Holidays), 07:00 – 17:15 Saturdays, Sundays, and Bank Holidays.
Service Level	99.99%
Increased Impact Service Level	99.60%
Significant Failure Service Level	99.00%

SL5 - Telephony Service Quality (MOS Score) –	
Service Level Description	A Service Level to measure the speech quality of inbound and outbound voice calls delivered by the PCI solution within a Calendar Month.
Service Level Calculation	The Mean Opinion Score of voice calls over a calendar month shall be measured at the point the calls pass in or out of the PCI Pal SBCs by using automated tools that calculate MOS CQ, E – (Mean Opinion Score Conversational Quality, Estimated) for all calls transiting the PCI solution. Where MOS scores are not achieved because of: • Round Trip Delay (WAN service) (If RTCP is available) • Jitter (WAN Service) • Packet Loss (WAN Service) • Other LAN/WAN issues the Supplier shall be liable for and resolve the issue with the LAN or WAN Providers unless the issue is diagnosed as being within the DWP call centre beyond the PCI Pal SD-WAN network termination point.
Agreed Service Time	This Service shall be available 24 hours per day, 365 days per year (366 days in a leap year).
Agreed Service Measurement Time	This Service shall be measured 07:00 – 21:00 Monday – Friday (excluding Bank Holidays), 07:00 – 17:15 Saturdays, Sundays, and Bank Holidays.
Service Level	Of the measured G.711 encoded calls transiting the PCI solution - 99% shall achieve a MOS score of 4.0 or greater - of the remaining 1%, 0.91% shall achieve a MOS score of 3.7 or greater.
Increased Impact Service Level	96% of measured calls transiting the PCI solution shall achieve a MOS score of 4.0 or greater.
Significant Failure Service Level	90% of measured calls transiting the PCI solution shall achieve a MOS score of 4.0 or greater.

SL6 – Payment Card Industry Customer Payments	
Service Level Description	A service level to measure the percentage of successful Payment Attempts and responses against the number of calls received. A Successful Response is when the Department is notified that the payment has been submitted to Gov Pay within 3 seconds of the request being made by the agent.
Service Level Calculation	Payment Card Industry Successful Notifications shall be calculated as a percentage of the total number of successful notifications submitted to the department within a response time of 3 seconds within a calendar month in accordance with the following formula: Service Performance = $\frac{(B-A)}{B} \times 100\%$ Where: A is the total number of successful notifications to the Department within a response time of 3 seconds of submission during the Calendar Month. B is the total number of payment requests made during the Calendar Month. Payment attempts to the payment gateway where no response is received from the payment gateway within 2secs will be excluded from the total number of payment requests.
Agreed Service Time	This Service shall be available 24 hours per day, 365 days per year (366 days in a leap year).
Agreed Service Measurement Time	This Service shall be measured 07:00 – 21:00 Monday – Friday (excluding Bank Holidays), 07:00 – 17:15 Saturdays, Sundays, and Bank Holidays.
Service Level	99.99%
Increased Impact Service Level	99.60%
Significant Failure Service Level	99.00%

Annex 2 – Service Credits

Two levels of service credits will be applicable, one for PCI card payment and one for telephony.

Where the Supplier fails to achieve any one of the specified Service Levels; Increased Impact Service Levels; or Significant Failure Service Levels, during any contracted calendar month, the Supplier will credit the Customer the percentage value of the monthly charges as set out below;

For clarity if more than one failure occurs the Supplier will only be accountable for a single failure in any one month and that being the highest impacted failure and related percentile value, i.e. Significant Impact Service Levels take precedence over the Increased Impact Service Levels and similarly Increased Impact Service Levels take precedence over Service Levels

If after three months of the same failed Service Level being achieved the Buyer may exercise rights to terminate for breach and may recover any previous or future investment associated with the service within any contracted year.

Should any individual Service Levels show a repeated trend of failing more than three times in any calendar year then the Supplier must provide a detailed remedial action and service improvement plan articulating the steps to be taken, at its own cost, to make the service stable such that it will meet the Service Levels.

A Telephony outage will automatically negate any claim under the Pay Services Service Credit in the same incident, as the Payment Service cannot function without the telephony service being active. Telephony service credits will be applicable for failure to achieve SL1, SL2 & SL5 as defined in document in Annex 1.

Telephony Service Credits			
Applicable SLA	Service Level	Increased Impacted Service Level	Significant Failure Service Level
SL1, SL2, SL5	<99.99%	<99.60%	<99.00%
In any calendar Month	20% of the calendar monthly charge	30% of the calendar monthly charge	40% of the calendar monthly Charge
Service Credit	[Redacted]	[Redacted]	[Redacted]

Telephony service credits will be applicable for failure to achieve SLAs; SL3, SL4 & SL6 defined in Annex 1, where the customer is able to make and receive telephone calls but is not able to take secure payments.

[Redacted]

Multiple service credits may be applied in a single month up to a maximum of 40% of the Monthly fees.

Annex 3 – Key Performance Indicators

KPI 1 - Performance Monitoring Reports Provided on Time	
KPI Description	A measure of the timeliness of Performance Monitoring Report delivery within 4 working days of the Calendar Month end expressed as a percentage of Performance Monitoring Reports for a Calendar month provided by the Supplier to the Buyer within the timescales.
KPI Calculation	A / B x 100% where: A = The number of Performance Monitoring Reports delivered within the KPI agreed timescales in the Calendar Month in question. B = The total number of Performance Monitoring Reports delivered in the Calendar Month.
Reporting Period	Service Measurement Period
KPI Measure	100% of Performance Monitoring Reports provided by the agreed date.

KPI 2 - Performance Monitoring of Applicable certifications	
KPI Description	A measure of maintenance of applicable compliance certifications as required by the Buyer: - ISO27001 Applicable PCI certifications Applicable Certifications that may apply to the Data Centre environments from where the Supplier delivers service to the Buyer. PCI Must provide a copy of the original certification within One month of the expiry of the current certification.
KPI Calculation	A / B x 100% where: A = The number of Applicable Certifications delivered within the KPI agreed timescales. B = The total number of Applicable Certifications delivered in the KPI agreed timescales.
Reporting Period	Service Measurement Period
KPI Measure	100% of Applicable Certifications provided by the agreed date.

KPI 3 - Service Provider Incident Resolution	
KPI Description	An STP (Service Tower Provider) is an entity in DWP Place that 1 or more related assignment groups can be mapped to. Service Provider Incident Resolution (formerly "GSO" Incident Resolution) is reported against the Service Provider, defined by the STP in DWP Place, that resolved the incident, and measures the cumulative amount of time, in New, In Progress or On Hold-Awaiting Vendor incident states only, that the incident spent assigned to any assignment group mapped to that resolving Service Provider/STP. This KPI provides Service Providers with a view of their own individual performance and is particularly useful for those incidents that have been assigned to more than 1 Service Provider. Although Service Provider Resolution is reported against the resolving STP, it is also possible to measure performance for any Service Provider that an incident was assigned to.
Automated DWP Place measure	Yes
KPI Start Point	The date/time that the incident is first assigned to a group mapped to the STP. Where there is an increase in incident priority, the measurement start point is either 1) the date/time at which the priority was increased (if assigned to the STP at that time), or 2) the date/time that the incident is next assigned to the STP after the priority increase has taken place, whichever happens sooner (refer to Measurement Hours section).
KPI End Point	Measurement ends when the incident is set to Resolved. Measurement pauses if the incident is reassigned to a group mapped to a different STP and recommences if the incident is reassigned back to the STP in question. Measurement also recommences if the incident is reworked, i.e. set back to In Progress state after having been set to Resolved and assigned back to the STP in question.
Target	Priority 1 = 90.00% in 2 hours Priority 2 = 95.00% in 8 hours Priority 3 = 95.00% in 20 hours (2 working days) Priority 4 = 90.00% in 30 hours (3 working days)
KPI Hours	Priority 1/2 = 24x7x365 (366 in leap year) Priority 3/4 = 08:00 - 18:00 Monday to Friday, excluding public holidays in England and Wales
Data Scope	**In Scope** • Incidents closed in the reporting period that were resolved by the Service Provider • All time that an incident spends in New, In Progress or On Hold-Awaiting Vendor states when assigned to the Service Provider.

	Out of Scope • No User Impact incidents (i.e. No User Impact tick box is checked), where there is no impact to the DWP customer and/or citizens • Child Incidents • Any time that an incident spends in any state other than New, In Progress or On Hold Awaiting Vendor states. • Any time that an incident spends assigned to an assignment group that is mapped to a different STP. • Any incident set to Cancelled state.
KPI Calculations	Performance achievement is measured separately for each Incident priority and is reported as a percentage. A / B x 100% where: A = Total No. Incidents closed in the reporting period resolved by the STP within target B = Total No. Incidents closed in the reporting period resolved by the STP
Reporting Source	Performance Analytics Dashboards (DWP Place)
Additional Rules/Notes	<u>Priority increase</u> If the priority of an incident is increased, the clock starts again. The measure calculation only includes the time spent assigned to the STP from the point that the priority is increased and is measured against the higher priority. <u>Priority decrease</u> If the priority of an incident is decreased, the clock does not restart. The measure calculation includes all the time spent assigned to the STP but is measured against the lower priority target.

KPI 4 - Incident Volume Reduction	
KPI Description	Continue to drive the overall reduction of Incidents experienced by users on their Digital products by a minimum of 10% (on previous year's figures).
Automated DWP Place measure	Yes
KPI Start Point	Not applicable
KPI End Point	Not applicable

Target	10% Reduction in 22/23 totals vs 21/22 totals (and subsequent years thereafter). Though an annual target, volume reduction will be monitored/reported monthly against the 10% target. Green: > 10% reduction Amber: > 5% - ≤ 10% reduction Red: < 5% reduction
KPI Hours	Not applicable
Data Scope	**In Scope** • User Incidents raised in the reporting period. **Out of Scope** • Proactive incidents (i.e. Proactive tick box is checked) where there is no impact to the DWP customer and/or citizens
Additional Rules/Notes	
KPI Calculations	Performance achievement is aggregated for all incident priorities and is reported as a percentage. Baseline = Total number of incidents raised in previous year (21/22) x100 Total number of user incidents raised in DWP Place Where the measure is reported monthly, or as a year to date figure, the baseline used is the total number of incidents raised for the same period the previous year.
Reporting Source	Performance Analytics Dashboards (DWP Place)

KPI 5 - Root Cause Analysis	
KPI Description	The number of Root Cause Analyses requested by the Buyer delivered within 10 Working Days of resolution of the Problem to which the analyses relate, and as accepted by the Buyer without material comments on analysis and proposed action plans, expressed as a percentage of the total number of Root Cause Analyses requested by the Buyer during the CALENDAR MONTH in question.
Additional Rules/Notes	**Average Time to Fix:** *Note these are not contractual measures but rather indicators / aspirational measures to assess Problem Performance so that action can be taken to review status and remove/address barriers to progression where appropriate. It is accepted that some Problems will take longer than these timelines to fix due to their complexity. Where Problems are not/cannot be fixed, this decision should be taken at the earliest appropriate opportunity.* ○ **Priority 1:** • Resolution/fix within 30 days

	○ **Priority 2:** • Resolution/fix within 60 days ○ **Priority 3:** • Resolution/fix within 80 days ○ **Priority 4:** • Agreed resolution/fix within 100 days *It is worth noting these measures are not based on Gartner but rather are a DWP Digital view based on analysis of performance data and trends over time.*
KPI Calculation	A / B x 100% where: A = The number of Root Cause Analyses requested by the Buyer delivered within 10 Working Days of the resolution of the Problem occurring in the CALENDAR MONTH in question, and as accepted by the Buyer without comment. B = The total number of Root Cause Analyses requested by the Buyer following resolution of the Problem and scheduled for delivery in the CALENDAR MONTH in question in accordance with the time limit stated above.
Reporting Period	Service Measurement Period.
KPI Measure	90%

KPI 6 - Software Release Implementation	
KPI Description	Percentage of Software Releases, Security Releases and Anti-Virus (AV) Software Releases and patches successfully installed within the applicable timescales set out below within a Service Measurement Period (CALENDAR MONTH)and in accordance with the IT Service Request Management Policy and Procedures or the Security Policies (as appropriate).
KPI Calculation	A / B x 100% where: A = The number of Software Releases, Security Releases andAnti-Virus (AV) Software Releases installed within the KPI Target timescales in the CALENDAR MONTH in question. B = The total number of Service and Security Releases and Anti-Virus (AV) Software Releases installed in the CALENDAR MONTH in question.
KPI Target	**Releases and Timescales:** Software Releases and Security Releases

	Standard Change A Standard Change is a change to a service or infrastructure for which the approach is pre-approved, relatively common and has an accepted established procedure to provide a specific change requirement. Has repeatable implementation steps with a proven history of success which are frequently implemented and does not require Service unavailability. Normal Change Normal Changes cover most Changes that require full assessment and authorisation. Normal Changes typically cover the following scope: • In response to business or user demands • To fix faults (Incidents or Problems) • To upgrade a system (e.g. a new release of software or hardware upgrade) • To introduce new (or remove old) Cis It is expected that Normal Changes are planned well in advance of implementation and will proceed in an orderly fashion through each stage of the process, including the Change Advisory Board (CAB), finally being implemented as part of the scheduled release. Emergency Change The 'Emergency' Change procedure is reserved for changes intended to repair an error in an IT service that is negatively impacting the business to a high degree. Emergency Changes should only be used when necessary. A Change is not an Emergency just because it has been poorly planned. Emergency Changes should only be considered where it is impossible to schedule a 'Normal or Standard Change' or there is an unavoidable risk to the Live environment if the Change is not implemented immediately, that is only when: • The Change resolves an Incident or Problem deemed critical to the business continuity where a work-around is not sufficient, this may include: • A Change forced by regulatory or statutory requirements which cannot wait until the next Change window; or • A Change addressing security requirements which can-not wait until the next Change window, or • A Change which needs to be applied to avert/mitigate a service-affecting Incident or to meet a business need **Anti-Virus (AV) Software Releases as follows:**

	(a) Emergency Anti-Virus Software Release – where there is a virus which in the opinion of the Supplier or the Buyer represents a real and present threat to the Buyer's business an Anti-Virus Software Release shall be installed on Payment Card Industry within 4 hours of the release becoming generally available to the market, or within timescales agreed with the Buyer. (b) Normal Anti-Virus Software Release – where a virus is known to be available on the Internet which in the opinion of the Supplier or the Buyer could have a significant impact on the Buyer's business but is not yet present on Payment Card Industry, an Anti-Virus Software Release shall be installed within twenty four (24) hours of the release becoming generally available to the market, or as agreed with the Buyer. (c) Normal Anti-Virus Software Release – Where an Anti-Virus signature file that has become available to the market to address known viruses shall be installed within forty eight (48) hours of the release becoming generally available to the market, or within timescales agreed with the Buyer.
Reporting Period	Service Measurement Period
KPI Measure	95%

KPI 7 - Billing Management Information Reports Delivery and Accuracy	
KPI Description	A measure of the overall accuracy of the Billing Management Information Reports as delivered to the Buyer within 10 days of the end of the calendar month.
KPI Calculation	Accuracy of the Billing Management Information Reports for each Calendar Month shall be measured by: Subtracting the total volume of errors attributable to the Supplier in the Invoicing Query Log for the Calendar Month from the total number of invoices raised in the Calendar Month as listed on the "Total Invoices Report". This shall be expressed as a percentage of the total number of invoices raised in the Calendar Month as listed on the "Total Invoices Report" i.e. % accuracy of Billing Management Information Reports for the Calendar Month = (A-B) / A x 100 where **A =** the total number of invoices raised in the Calendar Month as listed on the "Total Invoices Report" and **B =** the total volume of errors attributable to the Supplier in the Invoicing Query Log for the Calendar Month. Invoice and/or the Billing Management Information errors shall include but not be limited to:

	• Billing Management Information Reports not delivered within ten (10) Working Days of the Calendar Month end date • Invoice and associated Billing Management Information Reports not delivered at the same time • Invoice volume which does not match the Billing Management Information Reports volume • Activations/deactivations for a Resource Unit failing the opening / closing volumes reconciliation for the Calendar Month • Any reported usage of Resource Units at closed Sites • Errors in Site location code, business unit or cost centre that are attributable to the Supplier • Invoices raised for Services which the Buyer is disputing.
Reporting Period	Service Measurement Period
KPI Measure	99%

KPI 8 - Time to Publish Knowledge Articles	
KPI Description	Knowledge Articles provided by the Supplier within required timescales.
KPI Calculation	(A / B x 100) - C A = is Number of Knowledge Articles provided by the Supplier in the Calendar Month which are within seven (7) days of a Problem being Assigned to the Supplier B = Number of Problems Assigned to the Supplier for which a Knowledge Article was due to be provided by the Supplier within the Calendar Month C = if the Supplier fails to raise a Knowledge Article in respect of a Problem for which a Knowledge Article is required within fourteen (14) days (where the Knowledge Article was due in this or the preceding Calendar Month) C = 0 otherwise **Minimum Volumes** If there are less than ten (10) Knowledge Articles due in the Calendar Month, the KPI Measure shall be deemed met, provided that such Knowledge Articles shall be carried forward into the following Calendar Month or Calendar Months, until such time as there are ten (10) or more Knowledge Articles provided in a Calendar Month, at which point the KPI calculation shall then be carried out.

Reporting Period	Service Measurement Period
KPI Measure	90%

KPI 9 - Successful Change Management	
KPI Description	Measurement of the overall effectiveness of the Changes deployed by the Supplier within a Calendar Month.
KPI Calculation	A / B x 100 where: A = the aggregate number of Changes successfully deployed by the Supplier during each Service Measurement Period B = the aggregate number of Changes deployed (both successfully and unsuccessfully) by the Supplier during each Service Measurement Period. The definition of what constitutes a successful change are defined in the Change Management Policies and Procedures.
Reporting Period	Service Measurement Period
KPI Measure	Contract Year 1: 98.5% Contract Year 2: 99.0% Contract Year 3 onwards: 99.5%

Schedule 1: Services

Scope

No.	
001	The Supplier shall plan, design, test, install and manage a fully compliant PCI-DSS solution for taking card payments over the phone, delivering a fully integrated product. Compliance always required to latest current version of PCI-DSS.
002	The Supplier shall provide a solution that will work with the existing infrastructure.
003	The Supplier shall include all physical infrastructure, licences, and software as necessary to deliver such functionality. The Service to be called Payment Card Industry (PCI) and shall De-scope the Contact Centre on both inbound and outbound calls, across both CMG & Debt Management
004	The Supplier shall integrate to the payment systems in use i.e.: • Worldpay • Atos / SIEBEL • GovPay • AllPay
005	The Supplier shall describe the proposed solution in such a way that the commercial offering is clear e.g. • Customer Premise Equipment i.e. hosted by the department • Service based model i.e. the department rents the service • Hosted i.e. hosted by the Supplier but owned by the department • etc.
006	The Supplier shall provide design documents describing how the new solution will be implemented and managed.
007	The Supplier shall as a minimum ensure that sufficient capacity exists within the network to allow 10% over the maximum concurrent agent capacity
008	The Supplier shall ensure that PCI solution is fully integrated with all telephony services i.e. the departments Next Generation Contact Centre (NGCC) to meet the appropriate business strategies.
009	The Supplier shall ensure the operating environment and underlying service build parameters shall not impose any limitations on the delivery of the preferred solution
010	The Supplier shall ensure that periodic tasks required under PCI shall be conducted. This includes, but not limited to: • Annual Audit and Certification of the platform • Annual Audit and Certification of Support Services • Appropriate periodic scanning by an Assured Scanning Vendor • Appropriate monitoring and application of patches • Appropriate Monitoring, Alarming and Alerting of the platform • Appropriate Incident Management for items such as hacking attempts, breaches etc. • Any further evidence to ensure that PCI-DSS compliance is met
011	The Supplier shall provide the following services and functionality to ensure PCI-DSS compliance for taking card payments over the phone: The Service structure for the preferred solution is a blend of Business Groups for PCI-DSS. Service structure will include Inbound and Outbound calls for any Business Group including any systems that take card payments across the whole network
012	The Supplier shall supply a solution that masks Payment Card data, and in the future may be used to capture other numeric data including Bank Account details for Direct Debit mandates
013	The Supplier shall provide details of any applicable patents regarding the technology they provide

014	The Supplier shall provide details of any applicable licences regarding the technology they provide
015	The Supplier shall indemnify the Buyer in the event of a patent challenge
016	The Supplier shall ensure continued maintenance of applicable PCI Council obligations to ensure that they remain certified for the duration of the contract for: • PA-DSS • PCI-DSS • Service Provision This will include any new obligations introduced by the PCI council under subsequent revisions of the application PCI standards
017	The Supplier shall detail all components used in the solution or service
018	The Supplier shall detail the sourcing supplier for all components used in the service or solution
019	The Supplier shall detail the location of any development personnel outside of the UK
020	The Supplier shall detail the location of any support personnel outside of the UK

Usage

No.	
001	The Supplier shall confirm it has the necessary available capacity and capability to manage and process forecasted call volumes.
002	The Supplier shall confirm it has the necessary available capacity and capability to manage and process forecasted payment transaction volumes
003	The Supplier shall confirm it has the necessary available capacity and capability for staffing volumes if the concurrency is assumed to be at 76%.
004	The Supplier shall describe its ability to handle payments via inbound calls and provide call flows and payment data flow diagrams
005	The Supplier shall describe its ability to handle payments via outbound calls and provide call flows and payment data flow diagrams
006	The Supplier shall describe any modifications required on any of the infrastructure elements that make up NGCC e.g. • Sessions Border Controllers • SIP Components • Genesys Components including logging and attached data
007	The Supplier shall describe the transport mechanism for DTMF tones if DTMF tones are used for payment
008	The Supplier shall describe its ability and experience working with Genesys
009	The Supplier shall describe its ability and experience working with BT SIP trunks
010	The Supplier shall describe its ability to integrate with Payment Providers and supply a list of existing integrations
011	The Supplier shall describe its ability to integrate with Worldpay
012	The Supplier shall describe its ability to integrate with GOVPay
013	The Supplier shall describe its ability to integrate with Atos Payment Solution
014	The Supplier shall describe its ability to integrate with AllPay Payment Solution
015	CMS2012 is integrated with the card payment processor (ATOS) and that integration must be retained to avoid impact on the caseworker/client experience. For information the process is as follows, starting at the point that a client wants to make a card payment during a telephone call (both inbound and outbound): • Payment details are sent to ATOS via a web service. Details included in the request include Merchant id and Customer id. • The current response is URL which is used to redirect the case worker browser to the ATOS payment page. • Once the payment is complete ATOS redirects the browser back to Siebel • ATOS then calls a web service exposed by CMS2012 passing details of the payment received. This information is used to notify the client of a successful payment.

016	The Supplier shall describe and provide evidence of its compliance with PCI-DSS, PA-DSS and any other PCI compliance certifications
017	The Supplier shall describe its ability to select which card schemes are to be accepted e.g. accept VISA Credit / Debit, but exclude American Express
018	The Supplier shall describe its ability to check the card Primary Account Number (PAN) as it is entered e.g. LUHN check.
019	The Supplier shall describe its ability to support different transaction types e.g. Authorisation PAN, Authorisation PAN & CVV, Authorisation & Settle PAN / PAN & CVV etc.
020	The Supplier shall describe its ability for real time authorisation of transactions
021	The Supplier shall describe its approach to settlement and reconciliation
022	The Supplier shall describe its ability to support multiple Merchant ID's (MIDs)

Considerations

No.	Responsibility
001	The Supplier shall provision the solution to ensure the agent user interface can be displayed in both English and Welsh Language
002	The Supplier shall provision the solution to ensure capability to comply with 'The Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations 2018'. The 'common standards' DWP requires applications to meet are the Web Content Accessibility Guidelines version 2.1 to AA standard.
003	The Supplier shall provision the solution to ensure payments for multiple customers can be taken on a single call with no detriment to the current service provided
004	The Supplier shall provide a solution that enables the customer agent to keep the customer on the call during the payment process so that, open dialogue is maintained and, payments are confirmed. Full call recording must be maintained throughout and entry of card details obfuscation such that the card details cannot be obtained, or reverse engineered.
005	The Supplier shall supply any preferred solution including the design, test and installation and maintenance. Ensuring the solution is fully integrated and working to required specification
006	The Supplier shall supply a fully integrated solution to support business strategies and associated Management Information, minimising the potential of: • Unauthorised disclosure of Citizen information • Fines up to the limits under GDPR • Internal / external fraud opportunities • Agent temptation to commit fraud • Reputational damage to the Department
007	The Supplier shall describe how it will assist the Department in obtaining and maintaining compliance

Systems Used

No.	Responsibility
001	The Supplier shall ensure that the following systems are provisioned on the Payment Card Industry Solution: • World Pay • ATOS • AllPay • CMS 2012 • Workspace Inc. CS2, CSCS • Verint • BANcS
002	Upon request of the Department the supplier will: • Incorporate new 3rd party systems to ensure continuous PCI-DSS compliance • Protect any future Auto Pay self-service solutions

	• Remove or disable existing 3rd party systems that the Department doesn't use

Security Policy

No.	Responsibility
001	The Supplier shall provide support as required by the Department QSA during period audits as required under PCI
002	The Supplier shall ensure that all personnel working with the DWP are cleared to the appropriate security level i.e. BPSS
003	The Supplier shall ensure that personal with privileged access are cleared to SC level.
004	The Supplier shall allow and be subject to period visits by Department security personnel
005	The Supplier shall act upon agreed enhancements to security process and procedures as required by Department security
006	The Supplier shall be subject to physical audit and certification by Department security personnel
007	The Supplier shall describe its ability to conform to the department security policies, supplied in this pack.

Risks and QSA Report

No.	Responsibility
001	The Supplier shall ensure all agent dependencies are removed with the preferred solution
002	The Supplier shall provide ongoing support for the solution
003	The Supplier shall describe which items will be de-scoped from PCI-DSS and how this will be achieved
004	The Supplier shall describe what level of compliance will be achieved e.g. SAQA/B/C, etc.
005	The Supplier shall describe what level of compliance will be achieved if this is not SAQ.

Service Management

No.	Responsibility
001	The Supplier shall confirm that where obligations under PCI are better for the authority than those normally requested by the Buyer will take precedence.
002	The Supplier shall provide an automated integrated feed for providing Asset and Configuration Item (CI) data from the Supplier's system tool(s) into the Buyer's IT Service Management Tool DWP Place if asset and CI data is not managed directly in DWP Place
003	Tooling interface will be two-way with data being sent from the Supplier's CMS to an agreed schedule, cross-supplier brokered data made available to other suppliers and the Buyer's IT Service Management tools requesting information performance and availability data being sent from the Supplier's management system in near real time (or real time depending on commercial viability)
004	The Buyer and the Supplier will agree an Asset and CI Data Specification including, but not limited to a description of the in-scope Asset and CI frequency and expected volumes
005	Following go-live, the Buyer will hold review meetings with the Supplier on the Asset and CI data being passed. The Buyer reserves the right to request changes, if required, for a period of up to 6 SMPs after go-live (known as Tuning Phase). All changes in this period shall be subject to the Change Control Procedure.
006	The Buyer reserves the right to specify the 'discovery' utility. The Supplier will provide raw and unmodified Asset and CI data output from the discovery utility to the Buyer. Where the Buyer has specified the 'discovery' utility then the Buyer will bear the cost of the discovery utility licences. The Supplier will be responsible for implementation costs of the discovery utility.
007	The Supplier shall provide an automated integrated feed for availability and performance data from the Suppliers system tool(s) into the Buyer's IT Service Management toolset DWP Place and the Buyer's Application Performance Management (APM) tool.

008	The Buyer and the Supplier will agree an Availability and Performance Data Specification' including, but not limited to: a) the data that will be used to build the performance management database b) the events that will be triggered and passed to the Buyer's IT Service Management Toolset when the required service availability is at risk of failure c) how the data will provide evidence of achieved versus agreed availability and identification of areas where availability must be improved d) frequency and expected volumes
009	The Supplier shall provide an automated integrated feed for filtered system and other service impacting events from Supplier's system tool(s) into the Buyer's IT Service Management Toolset DWP Place and the Buyer's Application Performance Management (APM) tool.
010	Interface shall be one-way with events being sent from the Supplier's management system in near real time (or real time depending on commercial viability)
011	The Buyer and the Supplier shall agree an 'Event filtering and Correlation Rules Specification' including, but not limited to: a) the events that shall be passed into the Buyer's IT Service Management Toolset b) 1st and 2nd level correlation rules c) event types d) category e) frequency and expected volume
012	This will form an agreed monitoring baseline. Following go-live the Buyer shall hold review meetings with the Supplier on the filtered events being passed. The Buyer reserves the right to tune (i.e. ask for filtering to be applied) to the baseline for the period of the contract. Any extensions (or deletions) to the monitoring baseline shall be subject to the Change Control Procedure. To further support monitoring and performance transparency the Buyer reserves the right to: a) Measure, using probes, the real time application and service performance at key boundaries b) Read only access of core monitoring platforms to enable the download of historic data for analytics c) Receive any Incidents/Problems that would impact the Buyer not submitted through DWP Place but resolved within the Supplier environment
013	The Supplier shall perform IT Service Continuity Tests in accordance with the Buyer's IT Service Continuity Test Programme and resolve any issues that are discovered during the Tests
014	The Supplier shall review, update, and maintain IT Service Continuity Test Plans at least annually
015	The Supplier shall ensure all potential risks and threats to the Buyer's Live IT Estate are assessed, notified to the Buyer with details of how these shall be mitigated. Major risks or threats identified immediately, all others no later than 5 working days
016	The Supplier shall mitigate risk to the Buyer's IT Services by identifying any systems/applications which do not have Disaster Recovery in place and put a mitigation mechanism in place which ensures service continuity
017	The Supplier shall perform all required activities if an IT Service Continuity Event is declared
018	The Supplier shall enable the reduction in the end to end time taken to complete standard service requests
019	The Supplier shall provide and install items ordered and authorised within their contractually required delivery timescales
020	The Supplier shall, when required because of a Service Desk access request, provide user access to the System or Application as specified. Where possible the Supplier will work with the Buyer to introduce automatic fulfilment of approved Access request through automation with the Buyer's ITSM toolset DWP Place.
021	Where required, the Supplier shall change or remove End User access to systems and/or services in accordance with instructions from the Buyer in the timescales agreed

022	The Supplier will use the Buyer's IT Service Management Toolset DWP Place to manage and maintain the service and product catalogue request items.
023	The Supplier shall achieve all required Service Levels and KPIs each SMP and provide accurate supporting documentation to the Buyer to evidence this
024	The Supplier shall resolve any failures to meet Service Levels
025	The Supplier shall review Service Levels on an on-going basis and make recommendations to ensure the services continue to meet the Buyer's business needs
026	The Supplier shall use the Buyer's IT Service Management Toolset DWP Place for Service Level Management
027	The Supplier shall prior to any new or changed service going live provide the Buyer's Service Level Management team with an Operational Implementation Plan that meets the agreed quality standards and allows the service to be accurately measured
028	The Supplier shall provide impact assessment to new Policies and Procedures and changes to existing Policies and Procedures within required timescales
029	The Supplier shall undertake all activities required to ensure rapid on-boarding to the Buyer's Service Management Policies and Procedures
030	The Supplier shall resolve all Policies and Procedures non-compliances as soon as possible but no later than 3 reporting periods after the non-compliance has been raise.

Service Management - Security

No.	Responsibility
001	The Supplier shall support the security assurance audit (IT health check) contractor and the Buyer to organise and complete audits. This includes but is not limited to: a) providing access to all relevant resources such as, staff with sufficient knowledge of the subject matter of the audit, Supplier premises and relevant information b) liaising directly with the security assurance audit contractor to try to agree factual accuracy of non-compliances and observations. c) Agreement shall not be unreasonably withheld by the Supplier. A clear explanation must be provided to the security assurance audit Supplier for any non-agreement d) **c.** providing remedial actions with owners and completion dates to the Buyer for each non-compliance that is agreed not more than 10 working days following the agreement of factual accuracy
002	The Supplier shall support the IT health check contractor and Buyer to organise and complete IT health checks and Penetration Tests on the platform, including the Authorities Administration Portal and federated areas. This includes but is not limited to: a) providing all relevant resources such as physical and logical access, change procedures, relevant information, and key contacts b) liaising with the Buyer and the IT health check contractor to agree factual accuracy of findings c) providing an initial impact assessment within one working day for those vulnerabilities deemed critical by the Buyer and within 5 working days for all other vulnerabilities identified d) taking the necessary action, as agreed with the Buyer, to remediate vulnerabilities, unless agreed by the Buyer that the vulnerability shall not be remediated the Supplier's control
003	The Supplier shall support the security assurance vulnerability contractor and Buyer to organise and complete vulnerability scans. This includes but is not limited to: a) providing all relevant resources such as physical and logical access to systems and networks, change procedures, relevant information, and key contacts

	b) providing an initial impact assessment within 1 working day for those vulnerabilities deemed critical by the Buyer and within 5 working days for all other vulnerabilities identified c) taking the necessary action, as agreed with the Buyer, to remediate vulnerabilities, unless agreed by the Buyer that the vulnerability shall not be remediated which relates to the Authorities Administration Portal, and underlying platform, specifically relating to federated architecture.
004	The Supplier shall ensure all systems and software are supported by vendor security fixes. Vendor security alerts should be monitored for security alerts. Security fixes must be assessed for criticality and applied in accordance with the agreed patching policy
005	The Supplier shall ensure that all systems are adequately protected from the threat of malicious code of all types. Anti-virus and intrusion detection definitions and software must be kept up to date. Malware must be quarantined, and alerts triggered on detection. Security incidents must be raised when malware is detected.
006	The Supplier shall ensure that unauthorised devices are not connected to Buyer networks or attached to Buyer equipment. Authorised devices must be operated in accordance with security policies.
007	The Supplier shall support the Buyer regarding Security Incident Management. This includes but is not limited to: a) providing all resources, information and access required by the Buyer, or any third party appointed by the Buyer to complete the investigation b) establishing an effective security incident process and reporting mechanism c) as security incidents occur, the Supplier shall report immediately to the Buyer via the agreed security incident process d) maintaining accordance with GDPR requirements
008	The Supplier shall support the Buyer regarding forensic investigations. This includes but is not limited to: a) providing all relevant resources such as physical and logical Access to systems and networks, information, and key contacts b) physically securing or seizing equipment identified as evidence in a forensic investigation in such a way as to preserve its integrity in line with best practice
009	The Supplier shall support external subject matter experts and consultants representing the Buyer by providing reasonable and relevant information to the external party in a timely manner.
010	The Supplier shall ensure compliance with any applicable third-party agreement for connecting networks if appropriate
011	The Supplier shall ensure that all Supplier staff (including any sub-contractors) receive appropriate information security training (GSC, PCI etc) when joining the Supplier organisation. This includes but is not limited to: a) ensuring training is refreshed on an annual basis, maintaining the level of understanding of staff b) where appropriate include security awareness material supplied by the Buyer or authorised contractor(s) c) supporting the Buyer or authorised contractor(s) in the production of security awareness material specific to the Services
012	On receipt of security alerts or notices from the Buyer, the Supplier shall respond to the Buyer within agreed timescales detailing: a) actions already taken to mitigate the risk of such alert b) actions that will be taken to mitigate the risk of such alert and timescales

	c) reasons why such alert poses no risk to the Buyer
013	The Supplier shall take steps to identify all situations which pose possible or actual threats or vulnerabilities to the confidentiality, integrity and availability of systems, process, data, and people affecting the Buyer relating to the Services provided by the Supplier.
014	The Supplier shall support the Buyer's Protective Monitoring Service by sharing information such as threat intelligence, vulnerabilities, and less structured information, such as lessons learned reports, with the Security Operations Centre for situational awareness and tuning.
015	The Supplier shall support the Buyer's Protective Monitoring Service by establishing a Service Desk: a) protect security incident related data appropriate to its BIL (OFFICIAL in terms of classification but OFFICIAL-SENSITIVE for handling), in storage and in transit b) compartmentalise security incident related data (delegated management), providing access on a need to know basis c) authenticate user access to security incident related data appropriately
016	The Supplier shall work in compliance with the ISO 27001 information security management framework
017	The Supplier shall comply with all relevant legislation in terms of both operating and processing data on behalf of the Buyer
018	The Supplier shall Identify, document and review audit trails for systems which Buyer data is processed on, and inform the Security Expert Provider of any unusual or anomalous activity identified
019	The Supplier shall provide access to IT systems and data belonging to the Buyer as requested by the Department
020	The Supplier shall implement or utilise an existing means of providing accurate time in logs and synchronisation between system components with a view to facilitating collation of events between those components e.g. NTP
021	The Supplier shall take appropriate measures to secure both the internal and external boundaries of the system/solution provided to the Buyer by the Supplier, this may include but not be limited to, IDS, IPS, Firewalls and DLP
022	The Supplier shall provide Security Management Information and KPI reports as agreed upon within agreed timescales. The provision of Security Management Information could include statistics on but not limited to: a) Security Incidents b) Security Awareness c) Privileged Users d) In line with changes to PCI e) Audit Programme f) Clearance of staff such as Security Clearance, the following clearances must be in place prior to the commencement of the project: • Baseline Personnel Security Standard (BPSS) – Project / Account Resources • Security Check (SC Clearance) – for resources working with OFFICIAL information including any users with Privileged Access.
023	The Supplier shall obtain Cyber Essentials Certification to mitigate the risk from common Internet based threats
024	The Supplier shall provide details of any offshore development or applications hosting of their service
025	The Supplier shall ensure on-going compliance with all current and future security contractual obligations with which the Supplier must comply by: a) providing evidence to the Buyer on a scheduled basis to demonstrate compliance

	b) creating a corrective action plan to address identified areas of non-compliance and send the corrective action plan to the Buyer for approval. Such corrective action plan must include but is not limited to: • Actions to be taken to rectify the non-compliance • Timescales for such actions • Owners of such actions

Future Requirements

No.	Responsibility
001	The Supplier shall confirm capacity and capability for scalability this will include: a) Staffing increases b) Transaction increase c) System upgrades d) Changes to payment providers e) Self-Serve f) Business Continuity Planning g) Texbox h) SMS texting i) Scottish Devolution j) Brexit

Abbreviations

Abbreviation	Definition
PCI-DSS	Payment Card Industry Data Security Standards
SDM	Service Design and Management
CID	Customer Intelligence and Digital
NGCC	Next Generation Contact Centre
DM	Debt Management
CMG	Child Maintenance Group
HMRC	Her Majesties Revenue and Customs
DD	Direct Debit
SMI	Support for Mortgage Interest
GDPR	General Data Protection Regulations
CRU	Compensation Recovery Unit
TL's	Team Leaders
QSA	Qualified Security Assessor
ESRM	Enterprise Security & Risk Management
CL&D	Change Learning and Delivery
DWP	Department for Works and Pensions
IPT	Internet Protocol Telephony
DWP Place	The application used by the Buyer for Helpdesk purposes

Schedule 2: Call-Off Contract charges

The detailed Charges breakdown for the provision of Services during the Term will include the following items to cover Licensing, SD WAN and Racking:

[Redacted]

In addition, any outbound call charges will be charged on a per second basis in line with the current rate card (see Note 2 below) and will be payable each calendar month in arrears. These are estimated at £[Redacted] for Year 1 and £[Redacted] for Year 2, giving a total anticipated ContractValue for the 2-year term of **£3,320,434 excluding VAT**.

Notes:

1. All charges are expressed exclusive of VAT

2. No change to current rate card: "*PCI Pal Rate Card – DWP – Issue 1.0 (27-02-20)*"

3. Both licensing costs represent the total contract cost for system licensing and are inclusive of support

4. SD Wan (added as a Variation in October 2020 under the original contract) provides for custom power setup and cross connect

5. Racking (added as a Variation in June 2020 under the original contract) provides for data centre secure racking

The Buyer does not believe that Schedule 1 represents any change to the pre-existing business requirements and therefore expects that the current live service provided by the Supplier will satisfy this requirement, in line with the "*PCI Pal – DWP – Solution Design Document*".

Schedule 3: Enhanced Security Requirements

The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Buyer's security requirements as set out in the Contract which include the requirements set out in this Schedule 3 to the Contract (the "Buyer's Security Requirements"). The Buyer's Security Requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Buyer Assets, the Buyer's Systems Environment, and the Supplier's Systems Environment.

Terms used in this Schedule 3 which are not defined below shall have the meanings given to them in clause A1 (Definitions and Interpretations) of the Contract.

1. DEFINITIONS

1.1 In this Schedule 3, the following definitions shall apply:

"**Buyer Personnel**"	shall mean all persons employed by the Buyer including directors, officers, employees together with the Buyer's servants, agents, consultants, contractors, and suppliers but excluding the Supplier and any Sub-contractor (as applicable).
"**Availability Test**"	shall mean the activities performed by the Supplier to confirm the availability of any or all components of any relevant ICT system as specified by the Buyer.
"**CHECK**"	shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.
"**Cloud**"	shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data.
"**Cyber Essentials Plus**"	shall mean the Government-backed, industry-supported scheme managed by the NCSC with higher level of security requirements to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
"**Cyber Security Information Sharing Partnership**" or "**CiSP**"	shall mean the cyber security information sharing partnership established by the NCSC or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
"**Good Security Practice**"	shall mean: a) the technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for

Standardization or the National Institute of Standards and Technology);

b) security standards and guidelines relating to Information Security (including generally accepted principles regarding the segregation of the duties of governance, implementation, and control) provided to the public or Information Security practitioners and stakeholders by generally recognised authorities and organisations; and

c) the Government's security policies, frameworks, standards, and guidelines relating to Information Security.

"**Information Security**" shall mean:

a) the protection and preservation of:

i) the confidentiality, integrity and availability of any Buyer Assets, the Buyer's Systems Environment (or any part thereof) and the Supplier's Systems Environment (or any part thereof)

ii) related properties of information including, but not limited to, authenticity, accountability, and non-repudiation

b) compliance with all Law applicable to the processing, transmission, storage, and disposal of Buyer Assets.

"**Information Security Manager**" shall mean the person appointed by the Supplier with the appropriate experience, authority, and expertise to ensure that the Supplier complies with the Buyer's Security Requirements.

"**Information Security Management System ("ISMS")**" shall mean the set of policies, processes and systems designed, implemented, and maintained by the Supplier to manage Information Security Risk as certified by ISO/IEC 27001.

"**Information Security Questionnaire**" shall mean the Buyer's set of questions used to audit and on an ongoing basis assure the Supplier's compliance with the Buyer's Security Requirements.

"**Information Security Risk**" shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.

"**ISO/IEC 27001, ISO/IEC 27002 or ISO 22301** shall mean:

a) ISO/IEC 27001
b) ISO/IEC 27002/IEC
c) ISO 22301

in each case as most recently published by the International Organization for Standardization or its successor entity (the "**ISO**") or the relevant successor or replacement information security standard which is formally recommended by the ISO.

"**NCSC**"	shall mean the National Cyber Security Centre or its successor entity (where applicable).
"**Penetration Test**"	shall mean a simulated attack on any Buyer Assets, the Buyer's Systems Environment (or any part thereof) or the Supplier's Systems Environment (or any part thereof).
"**PCI DSS**"	shall mean the Payment Card Industry Data Security Standard as most recently published by the PCI Security Standards Council, LLC, or its successor entity (the "**PCI**").
"**Risk Profile**"	shall mean a description of any set of risks. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable.
"**Security Test"**	shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.
"**Tigerscheme**"	shall mean a scheme for authorised penetration tests which scheme is managed by USW Commercial Services Ltd.
"**Vulnerability Scan**"	shall mean an ongoing activity to identify any potential vulnerability in any Buyer Assets, the Buyer's Systems Environment (or any part thereof) or the Supplier's Systems Environment (or any part thereof).

1.2 Reference to any notice to be provided by the Supplier to the Buyer shall be construed as a notice to be provided by the Supplier to the Buyer's Representative.

2. PRINCIPLES OF SECURITY

2.1 The Supplier shall at all times comply with the Buyer's Security Requirements and provide a level of security which is in accordance with the Security Policies and Standards, Good Security Practice and Law.

3. ISO/IEC 27001 COMPLIANCE, CERTIFICATION AND AUDIT

3.1 The Supplier shall and shall procure that any Sub-contractor (as applicable) shall, obtain and maintain certification to ISO/IEC 27001 (the "**ISO Certificate**") in relation to the Services during the Contract Period. The ISO Certificate shall be provided by the Supplier to the Buyer on the dates as agreed by the Parties.

3.2 The Supplier shall appoint:

a) an Information Security Manager; and
b) a deputy Information Security Manager who shall have the appropriate experience, authority, and expertise to deputise for the Information Security Manager when s/he is on leave or unavailable for any period.

The Supplier shall notify the Buyer of the identity of the Information Security Manager on the Commencement Date and, where applicable, within 5 Working Days following any

change in the identity of the Information Security Manager.

3.3 The Supplier shall ensure that it operates and maintains the Information Security Management System during the Contract Period and that the Information Security Management System meets the Security Policies and Standards, Good Security Practice and Law and includes:

a) a scope statement (which covers all the Services provided under this Contract)
b) a risk assessment (which shall include any risks specific to the Services)
c) a statement of applicability
d) a risk treatment plan
e) an incident management plan

in each case as specified by ISO/IEC 27001.

The Supplier shall provide the Information Security Management System to the Buyer upon request within 10 Working Days from such request.

3.4 The Supplier shall notify the Buyer of any failure to obtain an ISO Certificate or a revocation of an ISO Certificate within 2 Working Days of confirmation of such failure or revocation. The Supplier shall, at its own expense, undertake those actions required in order to obtain an ISO Certificate following such failure or revocation and provide such ISO Certificate within one calendar month of the initial notification of failure or revocation to the Buyer or on a date agreed by the Parties. For the avoidance of doubt, any failure to obtain and/or maintain an ISO Certificate during the Contract Period after the first date on which the Supplier was required to provide the ISO Certificate in accordance with paragraph 3.1 (regardless of whether such failure is capable of remedy) shall constitute a Material Breach entitling the Buyer to exercise its rights under clause F5.2A.

3.5 The Supplier shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within 10 Working Days after completion of the relevant audit provide any associated security audit reports to the Buyer.

3.6 Notwithstanding the provisions of paragraph 3.1 to paragraph 3.5, the Buyer may, in its absolute discretion, notify the Supplier that it is not in compliance with the Buyer's Security Requirements and provide details of such non-compliance. The Supplier shall, at its own expense, undertake those actions required to comply with the Buyer's Security Requirements within one calendar month following such notification or on a date as agreed by the Parties. For the avoidance of doubt, any failure to comply with the Buyer's Security Requirements within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a Material Breach entitling the Buyer to exercise its rights under clause F5.2A.

4. CYBER ESSENTIALS PLUS SCHEME

4.1 The Supplier shall and shall procure that any Sub-contractor (as applicable) shall, obtain and maintain certification to Cyber Essentials Plus (the "Cyber Essentials Plus Certificate") in relation to the Services during Contract Period. The Cyber Essentials Plus Certificate shall be provided by the Supplier to the Buyer annually on the dates as agreed by the Parties.

4.2 The Supplier shall notify the Buyer of any failure to obtain, or the revocation of, a Cyber Essentials Plus Certificate within 2 Working Days of confirmation of such failure or revocation. The Supplier shall, at its own expense, undertake those actions required to obtain a Cyber Essentials Plus Certificate following such failure or revocation. For the

avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Plus Certificate during the Contract Period after the first date on which the Supplier was required to provide a Cyber Essentials Plus Certificate in accordance with paragraph 4.1 (regardless of whether such failure is capable of remedy) shall constitute a Material Breach entitling the Buyer to exercise its rights under clause F5.2A.

5. RISK MANAGEMENT

5.1 The Supplier shall operate and maintain policies and processes for risk management (the **Risk Management Policy**) during the Contract Period which includes standards and processes for the assessment of any potential risks in relation to the Services and processes to ensure that the Buyer's Security Requirements are met (the **Risk Assessment**). The Supplier shall provide the Risk Management Policy to the Buyer upon request within 10 Working Days of such request. The Buyer may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Buyer's Security Requirements. The Supplier shall, at its own expense, undertake those actions required to implement the changes required by the Buyer within one calendar month of such request or on a date as agreed by the Parties.

5.2 The Supplier shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Supplier's Systems Environment or in the threat landscape or (iii) at the request of the Buyer. The Supplier shall provide the report of the Risk Assessment to the Buyer, in the case of at least annual Risk Assessments, within 5 Working Days of completion of the Risk Assessment or, in the case of all other Risk Assessments, within one calendar month after completion of the Risk Assessment or on a date as agreed by the Parties. The Supplier shall notify the Buyer within 5 Working Days if the Risk Profile in relation to the Services has changed materially, for example, but not limited to, from one risk rating to another risk rating.

5.3 If the Buyer decides, at its absolute discretion, that any Risk Assessment does not meet the Buyer's Security Requirements, the Supplier shall repeat the Risk Assessment within one calendar month of such request or as agreed by the Parties.

5.4 The Supplier shall and shall procure that any Sub-contractor (as applicable) shall, co-operate with the Buyer in relation to the Buyer's own risk management processes regarding the Services.

5.5 For the avoidance of doubt, the Supplier shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this paragraph 5. Any failure by the Supplier to comply with any requirement of this paragraph 5 (regardless of whether such failure is capable of remedy), shall constitute a Material Breach entitling the Buyer to exercise its rights under clause F5.2A.

6. SECURITY AUDIT AND ASSURANCE

6.1 The Supplier shall and shall procure that any Sub-contractor (as applicable) shall, complete the information security questionnaire in the format stipulated by the Buyer (the "**Information Security Questionnaire**") at least annually or at the request by the Buyer. The Supplier shall provide the completed Information Security Questionnaire to the Buyer within one calendar month from the date of request.

6.2 The Supplier shall conduct Security Tests to assess the Information Security of the Supplier's Systems Environment and, if requested, the Buyer's Systems Environment. In

relation to such Security Tests, the Supplier shall appoint a third party which (i) in respect of any Penetration Test, is duly accredited by CHECK, CREST (International), or Tigerscheme and, (ii) in respect of any Security Test to which PCI DSS apply, is an approved scanning vendor duly accredited by the PCI. Such Security Test shall be carried out (i) at least annually, (ii) in the event of a material change in the Supplier's Systems Environment or in the Buyer's System Environment or (iii) at the request of the Buyer which request may include, but is not limited to, a repeat of a previous Security Test. The content, and format of any report of such Security Tests shall be approved in advance of the Security Test by the Buyer. The Supplier shall provide any report of such Security Tests within one calendar month following the completion of such Security Test or on a date agreed by the Parties. The Supplier shall, at its own expense, undertake those actions required to rectify any risks identified by any Security Test in the manner and within the timeframe required by the Buyer in its absolute discretion.

6.3 The Buyer shall be entitled to send the Buyer's Representative to witness the conduct of any Security Test. The Supplier shall provide to the Buyer notice of any Security Test at least one month prior to the relevant Security Test.

6.4 Where the Supplier provides code development services to the Buyer, the Supplier shall comply with the Buyer's Security Requirements in respect of code development within the Supplier's Systems Environment and the Buyer's Systems Environment.

6.5 Where the Supplier provides software development services, the Supplier shall comply with the code development practices specified in the Specification or in the Buyer's Security Requirements.

6.6 The Buyer, or an agent appointed by it, may undertake Security Tests in respect of the Supplier's Systems Environment after providing advance notice to the Supplier. If any Security Test identifies any non-compliance with the Buyer's Security Requirements, the Supplier shall, at its own expense, undertake those actions required in order to rectify such identified non-compliance in the manner and timeframe as stipulated by the Buyer at its absolute discretion. The Supplier shall provide all such co-operation and assistance in relation to any Security Test conducted by the Buyer as the Buyer may reasonably require.

6.7 The Buyer shall schedule regular security governance review meetings which the Supplier shall and shall procure that any Sub-contractor (as applicable) shall, attend.

7. PCI DSS COMPLIANCE AND CERTIFICATION

7.1 Where the Supplier obtains, stores, processes, or transmits payment card data, the Supplier shall comply with the PCI DSS.

7.2 The Supplier shall obtain and maintain up-to-date attestation of compliance certificates ("**AoC**") provided by a qualified security assessor accredited by the PCI and up-to-date reports on compliance ("**RoC**") provided by a qualified security assessor or an internal security assessor, in each case accredited by the PCI (each with the content and format as stipulated by the PCI and such reports the "PCI Reports"), during the Contract Period. The Supplier shall provide the respective PCI Reports to the Buyer upon request within 10 Working Days of such request.

7.3 The Supplier shall notify the Buyer of any failure to obtain a PCI Report or a revocation of a PCI Report within 2 Working Days of confirmation of such failure or revocation. The Supplier shall, at its own expense, undertake those actions required to obtain a PCI Report following such failure or revocation within one calendar month of such failure or revocation.

8. SECURITY POLICIES AND STANDARDS

8.1 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Security Policies and Standards set out Annex A and B.

8.2 Notwithstanding the foregoing, the Buyer's Security Requirements applicable to the Services may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the Services. Where any such change constitutes a Contract Change, any change in the Buyer's Security Requirements resulting from such Contract Change (if any) shall be agreed by the Parties in accordance with the Contract Change Procedure. Where any such change constitutes an Operational Change, any change in the Buyer's Security Requirements resulting from such Operational Change (if any) shall be agreed by the Parties and documented in the relevant Operational Change Confirmation.

8.3 The Supplier shall and shall procure that any Sub-contractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Standards.

9. CYBER SECURITY INFORMATION SHARING PARTNERSHIP

9.1 The Supplier shall be a member of the Cyber Security Information Sharing Partnership during the Contract Period. The Supplier shall participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information

9.2 The Supplier shall review the NCSC weekly threat reports on a weekly basis and implement recommendations in line with the Supplier's Risk Management Policy.

ANNEX A – AUTHORITY SECURITY POLICIES AND STANDARDS

The Security Policies are published on https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards unless specified otherwise:

a) Acceptable Use Policy

b) Information Security Policy

c) Physical Security Policy

d) Information Management Policy

e) Email Policy

f) Technical Vulnerability Management Policy

g) Remote Working Policy

h) Social Media Policy

i) Forensic Readiness Policy

j) SMS Text Policy

k) Privileged Users Security Policy

l) User Access Control Policy

m) Security Classification Policy

n) Cryptographic Key Management Policy

o) HMG Personnel Security Controls – May 2018
(published on https://www.gov.uk/government/publications/hmg-personnel-security-controls)

p) NCSC Secure Sanitisation of Storage Media (published on
https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

ANNEX B – SECURITY STANDARDS

The Security Standards are published on https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards:

a) SS-001 - Part 1 - Access & Authentication Controls
b) SS-001 - Part 2 - Privileged User Access Controls
c) SS-002 - PKI & Key Management
d) SS-003 - Software Development
e) SS-005 - Database Management System Security Standard
f) SS-006 - Security Boundaries
g) SS-007 - Use of Cryptography
h) SS-008 - Server Operating System
i) SS-009 - Hypervisor
j) SS-010 - Desktop Operating System
k) SS-011 - Containerisation
l) SS-012 - Protective Monitoring Standard for External Use
m) SS-013 - Firewall Security
n) SS-014 - Security Incident Management
o) SS-015 - Malware Protection
p) SS-016 - Remote Access
q) SS-017 - Mobile Devices
r) SS-018 - Network Security Design
s) SS-019 - Wireless Network
t) SS-022 - Voice & Video Communications
u) SS-023 - Cloud Computing
v) SS-025 - Virtualisation
w) SS-027 - Application Security Testing
x) SS-028 - Microservices Architecture
y) SS-029 - Securely Serving Web Content
z) SS-030 - Oracle Database
aa) SS-031 - Domain Management
bb) SS-033 - Patching

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 24 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 2 periods of up to 12 months each.

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 extend the contract beyond 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:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection
- 8.64 to 8.65 (Severability)

- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

2.2.2 a reference to 'CCS' will be a reference to 'the Buyer'

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

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

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

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

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

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

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

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

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

5. Due diligence

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

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

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

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

9.2.4 all agents and professional consultants involved in the Services hold employer's 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 Subject to clause 24.1 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 the Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. 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 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title, or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its Licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

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

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

11.5.2 Supplier's performance of the Services

11.5.3 use by the Buyer of the Services

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

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

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

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

11.7 Clause 11.5 will not apply if the IPR Claim is from:

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

11.7.3 other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy: https:/www.gov.uk/government/publications/government-security-classifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.cpni.gov.uk/content/adopt-risk-management-approach 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/technology-code-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 (and the Buyer of any Buyer Confidential Information breach). 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 is reasonable compensation and covers 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); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.89 to 8.90 (Waiver and cumulative remedies)

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

19.6 Each Party will return all the other Party's Confidential Information and confirm this has been done unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

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

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

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

21. Exit plan

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

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

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 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 extend the Term beyond 24 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 extension 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 the number of consecutive days set out in the Order Form, 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 4.2 to 4.7, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

24.1.1 Property: for all Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form

24.1.2 Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation, or damage to any Buyer Data, will not exceed the amount in the Order Form

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common

law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

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

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

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

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

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

29.6.1 its failure to comply with the provisions of this clause

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

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

29.8 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, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

Schedule 3: Collaboration agreement (Not used)

Not used

Schedule 4: Alternative clauses (Not Used)

Not used

Schedule 5: Guarantee (Not Used)

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 Section 2 (Services Offered) 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 Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: • owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation, and processes • created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.

Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data, and any information, which may include (but isn't limited to) any: • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably to 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 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 Framework Agreement 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)	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 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 including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other Default, negligence, or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
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-for-tax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: • acts, events, or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological, or chemical warfare • acts of government, local government, or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect, or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also

	includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.12 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 Section 2 (Services Offered) 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.
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.

Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium
Intellectual Property Rights or IPR	Intellectual Property Rights are: • 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	For the purposes of the IR35 rules an intermediary can be: • the supplier's own limited company • a service or a personal service company • a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	As set out in clause 11.5.

IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS'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, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
LED	Law Enforcement Directive (EU) 2016/680.
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 section 6 (What you report to CCS).

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 GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR.
Processor	Takes the meaning given in the GDPR.

Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:
	• induce that person to perform improperly a relevant function or activity
	• reward that person for improper performance of a relevant function or activity
	• commit any offence:
	  ○ under the Bribery Act 2010
	  ○ under legislation creating offences concerning Fraud
	  ○ at common Law concerning Fraud
	  ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication, and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.

Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
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 Section 2 (Services Offered) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Digital Marketplace.
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-check-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.

Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers, and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: GDPR Information

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

Annex 1: Processing Personal Data

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

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

2 [Redacted]

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

3 [Redacted]

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

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

Descriptions	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: ● *Related to the provision of the Secure Card Payment Service (SCPS)* **The Supplier is Controller and the Buyer is Processor** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data: ● *Not applicable* **The Parties are Joint Controllers** The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:

	● *Not applicable* **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: ● Business contact details of Supplier Personnel for which the Supplier is the Controller ● Business contact details of any directors, officers, employees, agents, consultants, and contractors of Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller ● *Related to the provision of the Secure Card Payment Service (SCPS)*
Duration of the Processing	*For the duration of the call of contract*
Nature and purposes of the Processing	*Provision of a cloud-hosted SCPS accessible over web by customer's call agents, able to receive form-entered information from call agent and intercept and capture DTMF from callers containing Payment Card data. Processes and transmits this data to customer's payment gateway and returns the transaction results, whilst keeping customer descoped from Payment Card data and PCI DSS requirements.*
Type of Personal Data	*Personal Data determined by customer, but must include at minimum telephony routing data and Payment Card data*
Categories of Data Subject	*Customer payment card data*
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	*Call and Payment Card data is held only in memory and destroyed promptly on end of call*

Annex 2: Joint Controller Agreement

Not used