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	Continuous Improvement and Support – 7560 4062 1125 157
Call-Off Contract reference	Supplier reference: SO017478
Call-Off Contract title	Digital Prisons – continuous improvement and managed cloud support
Call-Off Contract description	Continuous improvement and managed cloud support of Buyer's Digital Prisons Environments on the Azure platform, including developing testing and training environments for Digital Prisons
Start date	26th July 2021
Expiry date	25th October 2021
Call-Off Contract value	£455,000.00 + VAT (and expenses, if any)
Charging method	BACS
Purchase order number	To be confirmed on 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	Secretary of State for Justice on behalf of Her Majesty's Prison and Probation Services Buyer's main address: 102 Petty France London SW1H 9AJ
To the Supplier	Kainos Software Limited 02830571100 Supplier's address: Kainos House 4-6 Upper Crescent Belfast BT7 1NT Company number: NI019370
Together the 'Parties'	

Principal contact details

For the Buyer:
HMPPS Digital Contact
Title: Head of Technical Operations
[REDACTED]

Commercial Contact
Title: Commercial Manager
[REDACTED]

For the Supplier:
Title: Account Director
[REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 26th July 2021 and is valid for 3 months.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least 30 Working Days from the date of written notice for undisputed sums (as per clause 18.6).

	The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-off Contract can be extended by the Buyer for 1 period of up to 3 months, by giving the Supplier 4 weeks 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 3: Cloud support
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: • Continuous Improvement and Support, as per Service Offering 7560 4062 1125 157
Additional Services	Additional Services under this Call-Off Contract include: • Create test and training environments • Create new environment • Maintain the current Unilink technical backend infrastructure aligned with MoJ standards. • Keep the security standards aligned with MoJ requirement and industry best practices. This includes applying security patches / check for security vulnerabilities. • Apply software updates as per the business requirement working closely with Unilink. • Maintain Infrastructure Documentation and share any updates with MoJ Additional Cloud Services as required by the Buyer on a Time and Materials basis as per rate card. This may include but is not limited to: • ITIL-aligned ISO20000 certified operational support services which blends orchestration, automation, testing, continuous integration, continuous delivery (CI/CD) and defect resolution together to drive faster, safer, more frequent cloud deployments.

	• Kainos' Agile methodology and DevOps culture accelerate incident resolution, pipeline throughput, continuous delivery of product roadmap alongside continuous Improvement and support services.
Location	The Services will be delivered remotely or if agreed in advance between the Parties, from the Supplier's offices in the United Kingdom to the Buyer's address: [REDACTED]
Quality standards	The quality standards required for this Call-Off Contract are Digital by Default Service standards. • ISO 20000 IT Service Management • ISO27001 Information Security Management System standards. • NCSC guidelines
Technical standards:	The Supplier shall ensure the Services is aligned with ITIL v3. The Supplier processes are independently audited and accredited to ISO 20000 IT Service Management and ISO 27001 Information Security Management System standard. Any data gathered during the Call-Off Contract Term shall be retained only and processed only within the United Kingdom.
Service level agreement:	The Service level and availability criteria required for this Call-Off Contract are as set out below to the exclusion of the Service level agreement set out in the Kainos Support Services Terms and Conditions accessible from the catalogue here: https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92437/756040621125157-terms-and-conditions-2020-07-14-0849.pdf The Service hours are 0800 to 18:00 Monday to Friday excluding UK Bank Holidays. Support is provided via email and online support, and telephone support is also provided. Security Incidents: 99% of security incidents to be notified to ICT security team within 2 hours of a case being raised and a case is raised as a security incident. In calculating any incident response time, the calculation of time elapsed time will be suspended at the end of each working day until the next working day.

	[REDACTED]
Onboarding	The Supplier is the incumbent Supplier and therefore onboarding has already been completed.
Offboarding	The Offboarding Plan for this Call-Off Contract will be delivered as per the below: • The Supplier will hand over access to, and documentation for, the Buyer's Azure environments. • The Buyer is to remove the access for all Supplier staff who are providing these services to the Buyer to all Buyer and the Buyer's third-party providers' systems and the Buyer's Azure Infrastructure platform on the Contract End Date. • The Supplier is to support the transition of testing and training environment services, migration services and BAU services to the Buyer by the Contract End Date. Knowledge Transfer Requirements: The Supplier will work with the Buyer to facilitate all final exit management knowledge transfer requirements from the Supplier to the Buyer will be made at least 15 days in advance of the Call-Off Contract End Date. However, it is agreed that this shall take lower priority in line with the delivery requirements detailed above. Knowledge transfer includes (but is not limited to) the documents the Buyer specifies in their non-functional requirements, namely: • Design deliverables • Project plans • Analytical outputs • Reports • Visualisations • Lessons learned • Findings • Github Any additional offboarding requirements that are identified after the Contract Start Date are to be agreed in writing by both Parties at least 30 working days before the Contract End Date.
Collaboration agreement	N/A

Limit on Parties' liability	The annual total liability of either Party for all Property Defaults will not exceed 125% of the value of this call off contract. The annual total liability for Buyer Data Defaults will not exceed £1,000,000 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 £1,000,000 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 20 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 as per clauses 7.4 to 7.13 of the G-Cloud 12 Framework Agreement. 7.4 The Supplier will maintain full and accurate records and accounts, using Good Industry Practice and generally accepted accounting principles, of the: 7.4.1 operation of the Framework Agreement and the Call-Off Contracts entered into with Buyers 7.4.2 Services provided under any Call-Off Contracts (including any Subcontracts) 7.4.3 amounts paid by each Buyer under the Call-Off Contracts 7.5 The Supplier will provide a completed self audit certificate (Schedule 2) to CCS within 3 months of the expiry or Ending of this Framework Agreement. 7.6. The Supplier's records and accounts will be kept until the latest of the following dates:

7.6.1 7 years after the date of Ending or expiry of this Framework Agreement
7.6.2 7 years after the date of Ending or expiry of the last Call-Off Contract to expire or End
7.6.3 another date agreed between the Parties

7.7. During the timeframes highlighted in clause 7.6, the Supplier will maintain:

7.7.1 commercial records of the Charges and costs (including Subcon-tractors' costs) and any variations to them, including proposed varia-tions
7.7.2 books of accounts for this Framework Agreement and all Call-Off Contracts
7.7.3 MI Reports
7.7.4 access to its published accounts and trading entity information
7.7.5 proof of its compliance with its obligations under the Data Protection Legislation and the Transparency provisions under this Framework Agreement
7.7.6 records of its delivery performance under each Call-Off Contract, including that of its Subcontractors

7.8 CCS will use reasonable endeavours to ensure that the Audit does not unreasonably disrupt the Supplier, but the Supplier accepts that control over the conduct of Audits carried out by the auditors is outside of CCS's control.

7.9 Subject to any Confidentiality obligations, the Supplier will use reasonable endeavours to:

7.9.1 provide audit information without delay
7.9.2 provide all audit information within scope and give auditors access to Supplier Staff

7.10 The Supplier will allow the representatives of CCS, Buyers receiving Services, the Controller and Auditor General and their staff, any appointed representatives of the National Audit Office, HM Treasury, the Cabinet Office and any successors or assigns of the above access to the records, documents, and account information referred to in clause 7.7 (including at the Supplier's premises), as may be required by them, and subject to reasonable and appropriate confidentiality undertakings, to verify and review:

7.10.1 the accuracy of Charges (and proposed or actual variations to them under this Framework Agreement)
7.10.2 any books of accounts kept by the Supplier in connection with the provision of the G-Cloud Services for the purposes of auditing the Charges and Management Charges under the Framework Agreement and Call-Off Contract only

	7.10.3 the integrity, Confidentiality and security of the CCS Personal Data and the Buyer Data held or used by the Supplier 7.10.4 any other aspect of the delivery of the Services including to review compliance with any legislation 7.10.5 the accuracy and completeness of any MI delivered or required by the Framework Agreement 7.10.6 any MI Reports or other records about the Supplier's performance of the Services and to verify that these reflect the Supplier's own internal reports and records 7.10.7 the Buyer's assets, including the Intellectual Property Rights, Equipment, facilities and maintenance, to ensure that the Buyer's assets are secure and that any asset register is up to date 7.11 The Supplier will reimburse CCS its reasonable Audit costs if it reveals: 7.11.1 an underpayment by the Supplier to CCS in excess of 5% of the total Management Charge due in any monthly reporting and accounting period 7.11.2 a Material Breach 7.12 CCS can End this Framework Agreement under Section 5 (Ending and suspension of a Supplier's appointment) for Material Breach if either event in clause 7.11 applies. 7.13 Each Party is responsible for covering all their own other costs incurred from their compliance with the Audit obligations.
Buyer's responsibilities	The Buyer will: • Procure the cloud infrastructure as a Service and is responsible for any issues arising with that Service; • Provide all reasonably required access and administrative rights in respect of the Cloud Service as required by the Supplier to deliver the Services; • Comply with the Customer responsibilities in the Supplier Support Services Terms and Conditions accessible from the catalogue here: https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92437/756040621125157-terms-and-conditions-2020-07-14-0849.pdf All hardware required to run the Service, e.g. firewalls, or software installed above the hypervisor, e.g. specialist application backup software, or antivirus software will be owned by the Buyer. The Buyer will also:

	• Provide all reasonably required access to Buyer facilities and staff to deliver the Services, in particular with regard to onsite attendance by Supplier staff; • Provide all reasonably required access to third parties associated with the Services on which the Supplier is working. • Fulfil all management responsibilities of third parties. • Share all MOJ Security standards and policies required to be met by the Supplier with the Supplier upon the Contract Start Date. • Be responsible for providing the overall governance for the Buyer's infrastructure at these prison sites. • Provide guidance to the Supplier's Subject Matter Experts in how to effectively deliver these services.
Buyer's equipment	N/A

Supplier's information

Subcontractors or partners	N/A

Call-Off Contract charges and payment

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

Payment method	The payment method for this Call-Off Contract is BACS.
Payment profile	The payment profile for this Call-Off Contract is monthly in arrears.
Invoice details	The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to	Invoices will be sent to: [REDACTED] Post: Ministry of Justice Finance & Accounting

	Shared Services Connected Limited PO Box 766 Newport, Gwent NP20 9BB [REDACTED]

Invoice information required	All invoices must include:
	• Purchase Order Number
	• Contract Reference Number and Title
	• Cost Centre Code
	• Invoice Period
	• Details of charges for the invoice period, including:
	  ○ Which Services were provided for the invoicing period;
	  ○ The charges for each of these Services for the invoiced period;
	  ○ Each Service Role for the invoiced period;
	  ○ SFIA Level of each Service Role for the invoiced period;
	  ○ The number of days provided for delivering the Services for the invoiced period
	  ○ The start date for each Service role providing the services under the invoiced period
	  ○ The end date for each Service role providing the services under the invoiced period

Invoice frequency	Invoice will be sent to the Buyer monthly in arrears.
Call-Off Contract value	The total value of this Call-Off Contract is £455,000.00 + VAT (and expenses, if any)
Call-Off Contract charges	All effort will be charged on a time and materials basis for actual Supplier staff utilisation in accordance with Day Rates incorporated into the SFIA Rate Table below. The Supplier may agree to carry out work at the Location upon prior agreement from the Buyer that the Supplier can claim a flat rate of [REDACTED] for expenses per man day. [REDACTED] All charges in the table above are exclusive of VAT.

Additional Buyer terms

Performance of the Service and Deliverables	This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones: 1. Providing man days of Supplier effort on the infrastructure supplier services. It is agreed and acknowledged that at the time of contracting, the Supplier is using reasonable endeavours to recruit additional personnel to meet this requirement and shall keep the Buyer informed on progress. The Supplier shall not otherwise be held in breach of contract if it is unable to recruit and/or retain the desired personnel during the Call-Off Contract Term. 2. Support the installation and configuration of the Unilink Prison kiosks, biometrics and modules accessed via laptops (Web Client) and Staff modules Services onto the existing infrastructure for existing and agreed new sites. 3. The PaaS solution; work with MOJ and Unilink to develop and build the new environment based on a PaaS solution, including the production of relevant design document e.g. HLD, LLD. 4. The Test solution; work with MOJ and Unilink to support the development and build of the new environment based on a Test solution, including the production of relevant design document e.g. HLD, LLD. 5. The Training solution; work with MOJ and Unilink to develop and build the new environment based on a Training solution, including the production of relevant design document e.g. HLD, LLD. 6. Infrastructure clean of a significant amount of dead, unused and unknown infrastructure in the subscriptions the Supplier currently supports. This is to be cleaned up, re-documented and all none used items removed. The Supplier acknowledges that the Buyer is paying for the Services monthly and the Parties agree to work together collaboratively to provide Services as efficiently as possible. Once this is completed it needs to be documented at this point, allowing changes and further documentation to have a solid base. 7. Revisit the IaC (Infrastructure as Code) implementation, move to an open source and secret management system with a CI/CD Pipeline that fits the Buyer's standards. 8. Implement the new architecture design for data services. Follow RD Design to implement a new cost-effective SQL instance that will allow the infrastructure architecture to scale as and when required. 9. Revisit the RDS (Remote Desktop Services) implementation. Either scale or replace with another solution such as Azure Virtual Desktop. 10. To develop the API to link NOMIS and Azure Active Directory to satisfy the JML requirements, including all relevant design documents.
Guarantee	N/A

Warranties, representations	N/A
Supplemental requirements in addition to the Call-Off terms	a) It is agreed and acknowledged that under section 11.2 of the terms of this Call-Off Contract, 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. For the avoidance of doubt: a. all Background IPR and/or Project Specific IPR created during the Call-Off Contract Term in the Supplier's environments and any source code relating to the Buyer's Azure Prison Tenant Infrastructure, Test and Training environments, NOMIS APIs, deployment scripts, design documentation and SSLs shall be deemed to belong to the Supplier; and Any re-use/re-purpose of the above code or documentation by either party (done so in accordance with section 11.2 of the Call-Off Contract terms) shall not include disclosure of any configuration specific information.
Alternative clauses	N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms	N/A
Public Services Network (PSN)	N/A
Personal Data and Data Subjects	Annex 1 of Schedule 7 is being used

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	[REDACTED]	[REDACTED]

Schedule 1: Services

1. Services will be delivered by the Supplier to the Buyer for software environments at the below Buyer prison sites. The services shall be delivered to eleven (11) prison sites during the Term of the Call-Off Contract and are detailed in the following sections within this Schedule 1 (the “Services”).

[REDACTED]

Supplier staff roles which shall be utilised in the delivery of the Services to the Buyer shall include:

a. WebOps Designer
b. API Developer
c. Technical Architect
d. Application Developer
e. Client Services Manager
f. Service Delivery Manager

These requirements and services will be called off and charged in line with the SFIA Day Rate card, as included in Schedule 2 of this Call-Off Contract. WebOps Designer roles, Technical Architect roles, Application Developer roles, CSM roles and Service Delivery Manager roles shall be charged at SFIA Level 3-day rates as included in Schedule 2 of this Call-Off Contract. API Developer roles shall be charged at SFIA Level 4 day-rates, in line with the SFIA Day Rate card as included in Schedule 2 of this Call-Off Contract.

In-Cell Technology services - the Supplier shall lead the elements detailed below. The Supplier is responsible for the delivery of the below services:

a) Complete the testing and training environments
b) Complete the API between PNOMIS and AAD
c) Complete the design and build of the new PaaS environment
d) Create the cloud environment for new sites
e) Support and contribute to the transition approach and plan for new sites
f) Supply technical resources to help address issues as/when they arise during the deployments
g) Complete project management activities utilising existing service management staff, where possible.

[REDACTED] **- specific services:**

The Supplier is responsible for:

a. Data Migration activities, including (if applicable):
    a. Data cleansing
    b. Data manipulation (e.g. to enable move from v31 to v36 of the Unilink DB)
    c. Input into the development of the data migration approach
    d. Any other data related activities identified in the approach
b. Create the cloud environment for [REDACTED]
c. Input into the transition approach and plan for [REDACTED]
d. Supply technical resources to help address issues as/when they arise during the deployments. If the Supplier cannot provide technical resources within the timeframe requested by the Buyer, the Supplier must notify the Buyer immediately.
e. Supply of technical resources as required to address issues as they arise during the transition
f. Supporting project management activities utilising existing service management staff.

2. Business as Usual services:

a. In relation to the Buyer's Digital Prisons environments on the Azure platform, the Supplier will provide IaaS Support Activities as outlined in this contract subject to the assumptions, dependencies and Buyer Responsibilities and in acknowledgement of the risks detailed in this Schedule 1. Failure of any of the assumptions dependencies and Buyer Responsibilities outlined may affect the timely provision of the Services.

b. The Supplier will commence the Services in respect of Digital Prisons. Support for Digital Prisons will be provided on a time and materials basis.

c. The Supplier will provide the Buyer with continuous improvement support of the Digital Prisons Service, working through an agreed backlog provided by the Buyer. Continuous improvement support will be provided on a time and material basis.

d. As part of Managed Cloud Support Activities the Supplier will work with the Buyer (including managing competing priorities) to enable the Buyer's own team in working towards support of the Digital Prisons platform. The Buyer will determine the areas or functions and prioritisation of enablement activities.

e. The Supplier to facilitate proactive monitoring and alerting for the BAU services according with the MOJ Security Standards and policies at the time of contracting (which can be located at the following link https://security-guidance.service.justice.gov.uk/). The Supplier shall enact these requirements in collaboration with the Buyer's third-party supplier, Unilink Software Ltd.

f. Maintain the current Unilink technical backend infrastructure aligned with MoJ standards.

g. Keep the security standards aligned with MoJ requirements and industry best practices. This includes applying security patches / check for security vulnerabilities.

h. Apply software updates as per the business requirement working closely with the Buyer's third-party Supplier provider, Unilink Software Ltd.

i. Maintain Infrastructure Documentation and share any updates with MoJ such as HLD and LLD.

j. Supplier to provide monthly reports (as part of the monthly service report) of the current Buyer Prison Estate infrastructure with regards to license expiry, certificate expiry and patching status. Supplier to provide examples to the Buyer in the form of electronic confirmation.

k. The Supplier is required to participate in annual ITHCs if required within the term of the contract i.e. the provision of access to the Buyer's third party ITHC auditors.

l. Provision of suitably qualified resources to aid in fault identification and remediation for the Programme in relation to the Supplier services as provided under this Call-Off Contract, to the Buyer's third-party provider Unilink Software Ltd for all Unilink software services across the Buyer's Prison Estate, and the Buyer's third-party provider BT for networking services between the Buyer's Azure Prison Tenant Infrastructure, and BT PIN services in the Buyer's Azure cloud infrastructure and the Buyer's on-premise solution for PIN top up at HMP Cookham Wood.

Assumptions

a. The pricing and Services are contracted on the basis that no incumbent Supplier staff will transfer with the Service. In the event TUPE applies the Supplier reserves the right to revisit and revise the pricing on a reasonable basis to reflect additional Supplier cost associated with such TUPE transfer.
b. It is assumed that all components to be supported are delivered to Supplier's reasonable acceptable standard for Digital Prisons with no major reworking required to bring Services up to an efficiently supportable standard.
c. Where Buyer or third-party staff perform support activities, the Supplier has no liability for the performance of such tasks or the work undertaken by the Buyer or third-party staff.
d. For the purposes of this contract, it is assumed that there is one (1) supportable Service. Namely, Digital Prisons core infrastructure.

e. Buyer's Service management tool (currently ServiceNow) is capable of supplying the required reports to produce the monthly report. Supplier can only report on information available from the relevant tool.

Key Milestones:
The following milestones for this service delivery by the Supplier to the Buyer, to be completed in full by the Contract End Date, are listed below:

a. Providing man days of Supplier effort on the infrastructure supplier services, in accordance with the agreed resource profile.
b. Support the installation and configuration of the Unilink Prison kiosks, biometrics and modules accessed via laptops (Web Client) and Staff modules Services onto the existing infrastructure for existing and agreed new sites.
c. The PaaS solution; work with MOJ and Unilink to develop and build the new environment based on a PaaS solution, including the production of relevant design document e.g. HLD, LLD.
d. The Test solution; work with MOJ and Unilink to develop and build the new environment based on a Test solution, including the production of relevant design document e.g. HLD, LLD.
e. The Training solution; work with MOJ and Unilink to develop and build the new environment based on a Training solution, including the production of relevant design document e.g. HLD, LLD.
f. Infrastructure clean of a significant amount of dead, unused and unknown infrastructure in the subscriptions the incumbent currently supports. This is to be cleaned up, re-documented and all none used items removed. The Supplier acknowledges that the Buyer is paying for the Services monthly and the Parties agree to work together collaboratively to provide Services as efficiently as possible. Once this is completed it needs to be documented at this point, allowing changes and further documentation to have a solid base.
g. Revisit the IaC (Infrastructure as Code) implementation, move to an open source and secret management system with a CI/CD Pipeline that fits the Buyer's standards.
h. Implement the new architecture design for data services. Follow RD Design to implement a new cost-effective SQL instance that will allow the infrastructure architecture to scale as and when required.
i. Revisit the RDS (Remote Desktop Services) implementation. The Supplier is required to either scale, or replace with another solution such as Azure Virtual Desktop.
j. To develop the API to link NOMIS and Azure Active Directory to satisfy the JML requirements, including all relevant design documents.

3. ITIL Managed Service

The Supplier shall ensure the Services are aligned with ITIL v3. The Supplier processes are independently audited and accredited to ISO 20000 IT Service Management and ISO 27001 Information Security Management System standards.

The Supplier shall provide a named Service Manager to manage provision of the Services. The Supplier's Service Manager will deliver these services remotely. In addition to day-to-day interaction with their HMPPS Digital counterparts, the Service Manager will be responsible for monitoring ongoing quality of the Service. The Supplier proposes to use the current Service Design Package (SDP). The Supplier will review this document with the Buyer on a monthly basis and make any updates where required.

As per the Supplier's approach to date, the Service Manager will continue to distribute a monthly report and schedule a monthly Service review meeting.

The monthly Service report will continue to be produced in the current format. The report will continue to contain, but not be limited to, the following:

- Deliverables
- Uptime statistics
- Performance against KPI's and SLA's
- Incident counts
- Spend tracking
- Timesheet details
- Risks/Issues
- Continuous Improvement Items (Optional)

In addition, a named Senior Service Manager shall provide Service oversight and good practice Service management guidance as well as act as a point of escalation.

The Service management time for the Buyer support Services is charged on a T&M basis and billed monthly in arrears.

a. Key Features of Kainos' Managed Services

The key features of the Supplier's support Services include:

- Suppliers Service Desk – A reliable single point of contact into the Suppliers support team.

- Standard Service Hours – Standard hours of Service for the Supplier Staff are 08:00 to 18:00 GMT / BST, Monday to Friday, excluding UK bank and public holidays.

- Service Level Agreement – An agreed set of target response and resolution times by incident priority and classification defined in a Service level agreement (SLA) and as part of the agreed support contract.

- Escalation Process – An agreed escalation process will be defined. Agreed escalation process below. Subject to review and update upon contract signature. Escalation process to be reviewed as part of monthly service review.

[REDACTED]

- Third & Fourth Line Support –The Supplier provides end-to-end ownership of incidents, problems, Service requests and change requests.

b. Supplier Service Desk

[REDACTED]

- By email – [REDACTED] and a dedicated Digital Prisons support mail list [REDACTED]

- Online through the MOJ ServiceNow application.

- Direct contact details will be available to the Buyer's assigned Client Services Manager.

d. Service Level Agreement (SLA)

The current Digital Prisons Service support SLA has been detailed in the table below. This SLA has proven sufficient with the current support and the Supplier will abide by the below Target Response Times.

[REDACTED]

As per the current process, support tickets will be classified by HMPPS within ServiceNow based on the impact and urgency of the incident. The Supplier's engineers will prioritise resolution based on the priority assigned to any incident.

e. Security Clearance

The Supplier staff assigned to support Digital Prisons will have security clearance to a minimum of BPSS. Most Supplier staff will also already be cleared to SC level and the Supplier will seek to ensure all staff can achieve security clearance, should this be required. This will be monitored and agreed on a case by case basis.

Where necessary, the Supplier will obtain elevated security clearance for any additional support staff, via the Buyer, and apply appropriate process in the interim, e.g. in having personnel who are pending clearance work in the presence of those holding the necessary required clearance. The Supplier will request the Buyer's sponsorship for this.

f. Change and Release Management

The Supplier shall continue working under the current change and release management model, with the Buyer team having a named individual to control any and all changes and releases. The Supplier will continue to provide simplified, fit for purpose documentation to manage change and this will be coordinated through the MOJ ServiceNow application.

g. Service Transition

The Supplier understands the Buyer may transition live operations support for Digital Prisons into HMPPS Digital at the conclusion of this Call-Off Contract Term.

The Supplier will support this transition through the Service Manager, and other relevant staff, conducting a Service workshop covering all live operations Service activities, processes and technical aspects of Digital Prisons. The Supplier will work to the Buyers Service transition plan and will provide full input as and when required. In addition, and if required, the Supplier will also work with the Buyer's Digital team as part of their duties will capture knowledge gained from day to day activities or project work to such tools as confluence to ensure knowledge is shared and is completed to the Buyers satisfaction ahead of the planned end of this Call-Off Contract. This will include giving the Buyer's Digital team access to the code, build and infrastructure to apply fixes, fix problems (restart Services etc.) or carry out any proactive work as if they were a member of the Supplier's team. In the latter stages of the Call-Off Contract Term, the Supplier will work towards ensuring full enablement of the Buyer Digital team so that the transition from Supplier to Buyer Digital is seamless, thereby completing the Service transition.

In respect of knowledge transfer, the Supplier will provide all Digital Prisons documentation which the Supplier has been responsible for and which the Supplier continues to have in their possession. This includes (but is not limited to) the documents the Buyer specifies in their non-functional requirements, namely:

- Design deliverables
- Project plans
- Analytical outputs
- Reports

- Visualisations
- Lessons learned
- Findings
- Github

4. Approach for managing spend

a. Budget Optimisation and Flexibility

A key benefit of the Supplier's T&M pricing structure is that it gives the Buyer full flexibility to call upon the Services of the Supplier's team as and when required and only pay for that time that the Buyer uses. This 'pay as you use' approach means the Buyer can call upon as much / little of the Supplier support Services as required and continually adjust the amount of support the Buyer uses to meet their budget constraints.

The Supplier's team is already providing support to the Digital Prison Azure infrastructure, eliminating any requirement to upskill / familiarise another supplier with the infrastructure and application and the associated cost. The Buyer's team is already familiar with the Supplier's team and the Supplier's ways of working. Therefore, the Supplier can start delivering the support Services at pace through continuity of Service with no requirement to spend on any Service setup activity.

b. Continuous Budget Monitoring and Reporting

The Buyer's dedicated Service Manager will be responsible for reporting on Service performance. The report shall contain actual spend against budget. The Supplier continues to provide this granular level of financial detail on their monthly reports. Any significant variances in financial performance can be discussed during the monthly Service review meeting and the Service Manager will discuss options with the Buyer's team to ensure the spend must be the overall contract value.

Before working on any optional continuous improvement activity, the Supplier shall prepare an estimate on the number of hours required to complete each activity, from design to deployment. This will be agreed with the Buyer before the Supplier starts any development activity. Again, this will aid the Buyers decision-making process through enabling the Buyer to plan and prioritise what continuous improvements the Buyer wants implemented on the available budget.

c. Non-functional requirements

The following table details where the Supplier will comply with the Buyer's non-functional requirements:

Req. ID	High Level Business Requirement	Priority	Business Context / Notes	Kainos Response
Security				
AC1	The Supplier must assist MoJ Cyber group in operating, maintaining and continuously improving an Information Security Management System.	M		The Supplier shall comply with this requirement.
AC2	As the solution is Cloud-based, the Supplier will demonstrate compliance with the 14 cloud security principles.	M		The Supplier shall comply with this requirement.
AC3	The Supplier must demonstrate compliance with all applicable regulatory requirements, including but not limited to the Data Protection Act 1998.	M		The Supplier shall comply with this requirement.
AC4	The Supplier will comply with the marking and handling requirements for information as specified for OFFICIAL	M		The Supplier shall comply with this requirement.
AC5	The Supplier shall work with the Buyer Digital Studio Information Assurance team and make reasonable effort in order to ensure that the continuous assurance is in place and remains so.	M		The Supplier shall comply with this requirement.
AC6	Any connections into the Buyer's environment to support the solution shall not introduce additional unmanaged risks to the Buyer.	M		The Supplier shall comply with this requirement.
AC7	The Supplier shall ensure that all solution information is stored in areas with appropriate physical security controls for OFFICIAL.	M		The Supplier shall comply with this requirement.

AC8	The Supplier should provide boundary and gateway security controls at all system boundaries that are in accordance with NCSC published guidance and MoJ Hosting / Cyber practises at the time.	M		The Supplier shall comply with this requirement.
A9	The Supplier system should demonstrate how it will maintain the Confidentiality, Integrity and Availability of the data it processes.	M		The Supplier shall comply with this requirement.
AC10	All information/devices/equipment used for the solution shall be securely erased in line with commercial solutions required for OFFICIAL, to the approval of the Buyer information assurance. The Supplier shall provide evidence of such erasure and this shall be confirmed by a member of the Supplier organisation with sufficient seniority to take responsibility on behalf of the Supplier.	M		The Supplier shall comply with this requirement.
AC11	All equipment used to provide the solution shall be locked down, hardened and secured to in line with the OFFICIAL threat model	M		The Supplier shall comply with this requirement.
AC12	The Supplier should demonstrate defence in depth principles and appropriate segregation for the protection of information that aligns to the information value.	M		The Supplier shall comply with this requirement.
AC13	All personnel with access to the platform have as a minimum BPSS. Administrator/Privileged roles or those personnel in roles with additional privilege level must be holding SC.	M		The Supplier shall comply with this requirement.

AC14	All users of the solution systems data shall sign security operating procedures which explain the user responsibilities for information security and also require the user to positively acknowledge those responsibilities. The SyOps shall include the consequences of breaching the SyOps, which shall include disciplinary action, criminal prosecution and civil redress.	M		The Supplier shall comply with this requirement.
AC15	The Supplier shall ensure and demonstrate that only authorised and authenticated individuals are able to access the solution and that access is in line with relevant NCSC/MOJ guidance and standards	M		The Supplier shall comply with this requirement.
AC16	All bulk data movements shall be recorded in a Data Movement Form and shall have prior approval from the Buyer.	M		The Supplier shall comply with this requirement.
AC17	The Supplier should ensure that all data is subject to a backup procedure that is approved by the Buyer Digital Studio Information Assurance.	M		The Supplier shall comply with this requirement.
AC18	The Supplier should clear and sanitise any Digital Prison environment on request in line with relevant NCSC guidance and standards for OFFICIAL.	M		The Supplier shall comply with this requirement.
AC19	The Supplier must maintain the security patching and updates of all elements of the solution. Applying patches within agreed windows and in accordance to change control policies.	M		The Supplier shall comply with this requirement.

AC20	The Supplier should provide and maintain documentation that reflects the solution architectural design and security controls for review by the Buyer. Any changes shall be managed through a formal change control process which involves an assessment of Cyber implications of any change.	M		The Supplier shall comply with this requirement.
AC21	The Supplier should ensure and demonstrate that appropriate monitoring and detection controls are in place in order to identify possible information compromise within a timeframe aligned to the information value.	M		The Supplier shall comply with this requirement.
AC22	Any incidents, or suspected incidents involving the solution shall be reported to the Buyer as soon as the Supplier becomes aware of them.	M		The Supplier shall comply with this requirement.
AC23	The Supplier shall receive prior permission from the Buyer DS Cyber for any change to the solution environment which may impact the risks to the system.	M		The Supplier shall comply with this requirement.
Audit				
AT1	Any enhancements made by the Supplier will be consistent with GDS Digital Service Standard.	M		The Supplier shall comply with this requirement.
Audit				
AU1	The Supplier will ensure that the solution maintains controls that log and collect events, as specified in AU2 - 7 into a single place to support the detection of malicious activity.	M		The Supplier shall comply with this requirement.

AU1a	Ensure the solution continues to maintain controls that monitor malicious events and provide appropriate corrective actions.	M		The Supplier shall comply with this requirement.
AU1b	Ensure the solution continues to maintain any controls that prevent log information from being modified.	M		The Supplier shall comply with this requirement.
AU1c	Ensure the solution continues to maintain the controls to keep all its clocks synchronised to a common time source	M		The Supplier shall comply with this requirement.
AU2	Ensure the solution will continue to support the audit in place for all user accounts that are created, deleted, and changed.	M		The Supplier shall comply with this requirement.
AU3	Ensure the solution will continue to report all attempted transactions that fail due to security restrictions.	M		The Supplier shall comply with this requirement.
AU6	Ensure the solution will continue to record agreed events in an audit log accessible only to limited users.	M		The Supplier shall comply with this requirement.
AU7	Ensure the solution will continue to support the existing capture of: -the items of data being modified -the old value -the new value -the user modifying the data -the date+time stamp	M		The Supplier shall comply with this requirement.

AU8	Ensure the solution will continue to hold the audit data for an agreed retention period.	M		The Supplier shall comply with this requirement.
Availability				
AV1	The solution will maintain the availability level of 99.9% as specified in the cloud Service provider's Service definition.	M	The Supplier should be able to demonstrate in addition, the Recovery time objectives and Recovery point objectives. The Supplier should provide an architectural overview of the solution. The Supplier should provide a narrative supporting the Service levels of the solution.	The Supplier shall comply with this requirement.
AV2	The solution will be available 24 hours per day (P1 only), and will be configurable to automate out of hours shutdown of compute resources to agreed schedule.	M		The Supplier shall comply with this requirement.
AV3	The Supplier will provide a mechanism for managing incidents reported to them.	M		The Supplier can comply with this requirement. However, it is expected that the Buyer's ServiceNow will be the mechanism used.
Back up				

B1	The Supplier will support the solution data back-up controls ensuring conformance to the data back-up policy to prevent data from being permanently lost or corrupted following accidental or deliberate storage failures.	M		The Supplier shall comply with this requirement.
B2	If Supplier will support having a data aggregation prevention requirement it should provide back-up controls to prevent the data aggregated threshold being reached, the threshold defined within the solution business impact assessment (to be provided by the Buyer).	M		The Supplier shall comply with this requirement.
B3	Ensure the solution will continue to support data restore controls that restore data following data corruption/loss from previous back-ups in line with back-up policy to appropriately correct (recover) from a loss or corruption of Service.	M		The Supplier shall comply with this requirement.
B4	The Supplier will support the data back-up controls that conform to the data back-up policy (to be provided by the Buyer) to prevent data from being permanently lost or corrupted following accidental or deliberate storage failures.	M		The Supplier shall comply with this requirement.
Capacity				
C1	The Supplier will ensure the solution has capacity. Create views that show overall Service performance.	M		The Supplier shall comply with this requirement.
Design and documentation				

D1	All documentation produced and maintained will be made available to the Buyer and maintained on the Buyer's repositories.	M	This should include (but not be limited to): Design deliverables Project plans Analytical outputs Reports Visualisations Lessons learned Findings Github	The Supplier shall comply with this requirement.
Interoperability				
INT1	Interfaces with internal and external parties must be supported, maintained.	M		The Supplier shall comply with this requirement.
Performance				
P1	The Supplier will demonstrate and maintain the key performance indicators of the infrastructure – an agreed list of KPIs will be developed jointly at the outset. The Supplier should report against these indicators throughout the term of the Call-Off Contract.	M		The Supplier shall comply with this requirement.
Scalability				

SC1	The Supplier of the solution should be able demonstrate that the infrastructure scalability' is within tolerances. Recommendations will be given to the authority where savings or increases in computational resources, including processing power, memory, additional VMs, will be capable able to of being increased and reduced as required to meet fluctuations in demand, according to a utility pricing model.	M		The Supplier shall comply with this requirement.
Working collaboratively				
COL1	The Supplier will work seamlessly with Buyer staff who take over support of any aspect of the solution.	M	Including but not limited to; IaaS Support Application support Interoperability support	The Supplier shall comply with this requirement.

5. Assumptions

Area	Assumption
Commercial	• All costs will be invoiced monthly on a time and material basis • There are no 3rd party products requiring licenses or maintenance fees. • The Buyer will own, manage, and pay for the relevant Azure Subscriptions. • A support day is defined as 7.5 hours work completed between 08:00 and 18:00, Monday to Friday, excluding UK bank and public holidays. • All pricing is exclusive of VAT. • Services will be delivered from the Supplier's premises in the United Kingdom, primarily based in Belfast. • Should personnel be required onsite, a flat rate of £175 per staff member per day will apply to cover all travel and subsistence subject to be in line with MoJ Travel rates and policies.
Technical	• The Supplier has assumed that the Buyer has the necessary bandwidth to connect to the solution over the Internet. • The working area (confluence) for storing support Service and project documentation will be open to all team members (both Buyer and Supplier) to encourage collaboration. • Supplier team members will have access to the MOJ Digital slack as full members. • The Supplier will have access to the chosen backlog tool (Trello) • Security Considerations will be driven by the direction of Buyer security accreditor. • The Supplier assumes that the Buyer will continue to use ServiceNow for reporting all incidents and managing incidents.

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract.

The charges detailed in this Schedule are subject to the Pricing Assumptions set out at section 4 below.

1. Managed Cloud Support Activities

All effort will be charged on a time and materials basis for actual Supplier staff utilisation in accordance with the Rate Table below. The Supplier may agree to carry out work at the Location upon prior agreement from the Buyer that the Supplier can claim a flat rate of [REDACTED]

for expenses per man day.

It is expected that the delivery work will be carried out by WebOps Designer roles, Technical Architect roles, Application Developer roles, CSM roles and Service Delivery Manager roles, which shall be charged at SFIA Level 3-day rates. API Developer roles shall be charged at SFIA Level 4 day-rates. Where required, additional staff of SFIA day ratings 3-5 may be utilised to augment or replace the team to provide additional skills or for cost efficiency purposes. This will first be agreed by the Buyer and the Supplier via written confirmation (an email provided by the Buyer's designated Service Lead on behalf of HMPPS Digital to the Supplier's Primary Contact confirming the numbers of additional staff and any additional and/or amended charges is approved) is provided. The need for this will be reviewed and agreed on a regular basis.

2. All charges will be invoiced plus VAT monthly in arrears.

3. Rate Table
   [REDACTED]

The above rates are based on a 7.5 hour working day completed between the hours of 08:00-18:00 Monday to Friday, excluding UK bank holidays.

5. Pricing Assumptions
   a. Supplier reporting and transparency of charging will include:
      i. Monthly reporting will include a breakdown of staff activity Managed Cloud Support and continuous improvement against time and materials utilisation for Buyer review.
      ii. Charges in a given month will be time and materials costs.
   b. Team members will still be available to attend onsite by agreement, e.g. for upskilling, enablement, and any other Services to be taken on. It is not anticipated that a significant amount of on-site time will be required.
   c. There are no 3rd Party products requiring license or maintenance fees.
   d. The Buyer will own, manage and pay for the relevant Azure Subscriptions.

Customer Benefits

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

G-Cloud 12 Customer Benefits Record

Part B: Terms and conditions

1. Call-Off Contract Start date and length

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

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 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 employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

9.8.1 premiums, which it will pay promptly
9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 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 of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

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

20. Notices

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

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

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

21. Exit plan

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

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

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 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 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 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:
[REDACTED]

1.2 The contact details of the Supplier's Data Protection Officer are:
[REDACTED]

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

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

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: The Type of Personal Data under this Call-Off Contract will be: • The Custodial sentence terms, including the crime commit-ted, custodial sentence start date, custodial sentence end date, and name and location of prison/institution where the custodial sentence was is being served • Forenames, middle names, surnames, age, date of birth, gender identity, nationality, religion, ethnic group, • current and previous cell locations in prison/, of • Individual Offenders who are on remand or are serving a custodial sentence. • Account balance and 30 days of account transactions • Phone numbers of friends and family

	• Name, address, date of birth, phone numbers, biometric data of visitors • Biometrics data of offenders serving custodial sentences • Biometrics data of prison staff at prisons/institutions
Duration of the Processing	The applicable processing completed by the Supplier is running the back-up of the application data on a weekly basis. The back-up procedure occurs in an overnight process. This will take place for the duration of this Call-Off Contract. This final day of this action shall be the Contract End Date. If this Call-Off Contract is extended beyond the Exit Date, the final date for Processing HMPPS's Data will be agreed between the Buyer and the Supplier during the Call-Off Contract Extension period.
Nature and purposes of the Processing	Back-ups of the Digital Prisons CMS application occur on a weekly basis to ensure that in the event of an outage of a server or in the event on a major incident where the application's data is lost that data can be restored to a point in time up to a week previous. This data does not get edited by the Supplier in anyway. The Supplier will only backup the data within the azure environment
Type of Personal Data	The Type of Personal Data under this Call-Off Contract will be: • The Custodial sentence terms, including the crime commit-ted, custodial sentence start date, custodial sentence end date, and name and location of prison/institution where the custodial sentence was is being served • Forenames, middle names, surnames, age, date of birth, gender identity, nationality, religion, ethnic group, • current and previous cell locations in prison/, of Individual Offenders who are on remand or are serving a custodial sentence. • Account balance and 30 days of account transactions • Phone numbers of friends and family • Name, address, date of birth, phone numbers, biometric data of visitors • Biometrics data of offenders serving custodial sentences • Biometrics data of prison staff at prisons/institutions
Categories of Data Subject	• Individual Offenders who have served or are serving a custodial sentence. • HMPPS Prison staff members who are employed in the establishments which are in scope of this Call-Off Contract

	• Visitors for individual offenders who have served or are serving a custodial sentence
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	The backups created by the Supplier are retained for a week and replaced by the new backup taken. Once the processing of this Data is completed on the Call-Off Contract End Date, the Supplier and the Supplier's Subcontractor(s) shall destroy all Buyer data utilised or held by the Supplier or by any of the Supplier's subcontractors or partners in delivering these services under this Call-Off Contract within 5 working days after the Call-Off Contract End Date. Upon destroying the Buyer's data within this 5 working day period, the Supplier will provide the Buyer with a data destruction certificate relating to personal data destroyed by the Supplier within the time period agreed. If this Call-Off Contract is extended beyond the Exit Date, the final date for Processing Data will be agreed between the Buyer and the Supplier during the Call-Off Contract Extension period. Upon the confirming the final date for Processing Data during any Call-Off Contract extension period, the Supplier and the Supplier's Subcontractor shall destroy all Buyer data utilised or held by the Supplier or by any of the Supplier's subcontractors or partners in delivering these services under this Call-Off Contract within 5 working days after the final date for Processing Data. Upon destroying the Buyer's data within this 5 working day period, the Supplier will provide the Buyer with a data destruction certificate relating to personal data destroyed by the Supplier within the time period agreed.