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	843642414370275
Call-Off Contract reference	CON_XXXXXX
Call-Off Contract title	Self-Service Kiosks and associated services for prisoners and prison staff in HMPPS Public Prisons
Call-Off Contract description	Provision of self-service kiosks, including software modules, software support and maintenance, and leasing and maintenance of kiosks, and software and software maintenance for Unilink modules on in-cell technology, for use by prisoners and prison staff for up to 27 HMPPS public prisons for HMPPS Digital Prisons.
Start date	16th April 2021
Expiry date	15th April 2022
Call-Off Contract value	£3,520,000.00 The value above excludes VAT.
Charging method	BACS
Purchase order number	To be provided upon 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	The Secretary of State for Justice on behalf of Her Majesty's Prison and Probation Service The Ministry of Justice 102 Petty France London SW1H 9AJ
To the Supplier	Unilink Software Limited "Unilink" Supplier's address: Registered Address: Europoint, 5 Lavington Street, London SE1 0NZ Company number: 2924046
Together the 'Parties'	

Principal contact details

For the Buyer:
Title: HMPPS Digital Service Lead
[REDACTED]

Title: Commercial Manager
[REDACTED]

For the Supplier:
Title: Account Director
[REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 16th April 2021 and is valid for 12 months.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of 60 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 2 period(s) of up to 6 months each, by giving the Supplier 8 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 as per the Supplier's Service Offering 843642414370275 under: • Lot 2: Cloud software
G-Cloud services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: • Deliver the Custodial Management System CMS and combined biometric case management and self-service. • Hardware and software support for Kiosks and peripheral devices
Additional Services	The following additional services will be required on the 12 new In-Cell sites: • Site Survey • Kiosk Installation • Kiosk configuration • Reception Set up • Installation & configuration of peripheral devices • Azure set-up • Training support • Programme support
Location	The Services will be delivered at the following locations: [REDACTED]

	[REDACTED] The following public prisons will also receive these services: [REDACTED] All Buyer data used for the provision of these services under this Call-Off Contract will remain within the United Kingdom. The Supplier's datacentre security standards must comply with the CSA CCM version 3.0 standard, or equivalent standard.
Quality standards	The quality standards required for the Supplier to meet to provide these services to the Buyer under this Call-Off Contract are called out below: • All Supplier staff roles shall hold Counter Terrorism Clearance (CTC) • All Supplier Staff, and any of the Supplier's subcontractors and partners providing services to the Buyer under this Call-Off Contract with access to HMPPS Data shall hold Security Clearance (SC).
Technical standards:	The technical standards required for the Supplier to meet as a requirement for this Call-Off Contract are: • IT Health Check as completed at CHECK level • ISO27001 accreditation • Cyber Essentials Plus • ISO9001 principles • Conform to CESG CPA Build Standard • Comply with principles of ISO/IEC 27034 • Security governance certification • ITIL Change process • FIPS-assured encryption • Secure containers, racks or cages • Unilink's test and development networks meet IL3 level standards and can hold production data for a temporary period on a secure network • Data sanitisation type is explicit overwriting of storage before reallocation • Equipment disposal must comply with a recognised standard, such as CSA CCM v.30, CAS (Sanitisation) or ISO/IEC 27001 • Data Protection between Buyer and Supplier networks, and data protection within the Supplier network, will operate at the following standards: o TLS (version 1.2 or above)

	○ Legacy SSL and TLS (under version 1.2) • Have full and up to date continuity management plans which have been independently audited and may be provided to the Buyer upon request. • Configuration and change management standard must conform to CSA CCM v3.0 or an equivalent recognised standard • Vulnerability management type conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402. Unilink employs independent security consultants and work closely with supply chain partners such as Microsoft and Cisco to assess potential threats and implement mitigation measures including emergency patch deployment where advised to do so.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract for each of the three prison types are called out in further detail in Schedule 1 below. This section provides a high-level overview for the provision of these services. **Performance Reporting** • Attendance at three MoJ Checkpoint Meetings on a monthly basis. These are: ○ Once monthly Service Management to manage live sites. This may include (but is not limited to) information relating to incidents, changes, and performance of the service; ○ Once monthly programme meeting to manage deployment for the In-Cell Technology Programme. This may include (but is not limited to) information relating to deployment progress, challenges, and potential barriers in the In-Cell Technology Programme; ○ Once monthly Commercial and Contract meeting to discuss any issues that arise. This may include (but is not limited to) contract spend on deployment, software and hardware support, and repairs to hardware. • Provision of monthly status reports, with a follow-up service review if necessary. In addition to the above services the following support services will be required to be available to be called upon as required:

	The Buyer is establishing product teams, once the product teams are established, the Buyer will have the option to transfer support in-house under CCN process. Both Parties will at this point will have the option to renegotiate the operations costs based on the transfer of support. It is envisaged that 3rd line support would remain with the Supplier. In the event of any disaster (such as critical system failure of Unilink staff IT network, Unilink's services under this Call-Off Contract will be fully operational within 24 hours.
Onboarding	The Onboarding Requirements for this Call-Off Contract will be different for each prison type under this Call-Off Contract, which includes the following types of prisons: • Standard Prisons • Digital Prisons • In-Cell Digital Prisons The full list of onboarding requirements for each of these types of prisons is outlined in Schedule 1, Schedule 2, Schedule 3 and Schedule 4 of this Call-Off Contract, as below. The Suppliers' Project Management team will co-ordinate with the MoJ appointed contacts to arrange site visits, meetings, training and a complete range of on-boarding activities including work streams as defined to achieve a range of activities to meet MOJ requirements.
Offboarding	This is the offboarding of the Supplier's hardware and software services from HMPPS prison sites. During the term of this Call-Off Contract, the Supplier must: • Maintain a register of all of the Assets under the contract, including hardware and software, for each prison in scope of this Call-Off Contract; • Maintain a register of all technical infrastructure through which the software and hardware services are provided and how these services are maintained at all prisons in scope of this Call-Off Contract; • Maintain a register of all Buyer Data contained in the Supplier's system (a full list of the Buyer Data contained in the Supplier's system is as defined in Schedule 7 of this Call-Off Contract).

	HMPPS Digital on behalf of the Buyer may request that the Supplier may provide the information included in the above three registers to the Buyer during the Call-Off Contract. The Supplier is to share the above information with the Buyer within 5 working days of the Buyer's request being received by the Supplier. The Supplier shall submit an Exit Plan to the Buyer for Approval within three (3) months after the Call-Off Contract Start Date, which sets out the Supplier's proposed methodology for achieving an orderly transition of Services from the Supplier to the Buyer and/or its Replacement Supplier(s) on the expiry or termination of this Call-Off Contract. The Exit Plan shall include (but is not limited to): • Specific processes for exit management from each of the three prison types (Standard Prisons, Digital Prisons and In-Cell Digital Prisons respectively). This includes the management structure to be put in place and employed during the exit management period for each of these three prison types (Standard Prisons, Digital Prisons and In-Cell Digital Prisons respectively). • Full details of timescales, activities, and roles and responsibilities for each of the Parties under this Call-Off Contract, for: o 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. o The strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer and/or a Replacement Supplier, including conversion to open standards or other standards if required by the Buyer. This includes the Supplier's provision of data migration support to the Buyer for each of the three prison types (Standard Prisons, Digital Prisons and In-Cell Digital Prisons respectively). This includes any timelines for the data migration, and any potential costs for the Supplier's provision of data migration support to the Buyer that may arise during this exit management period. The designated point of contact at HMPPS Digital on behalf of the Buyer will provide support to the Supplier if required to define the main milestones for

	these exit management arrangements and deadlines for completion at each of the Buyer's prison sites. The Buyer is responsible for defining the standards for the exportation and migration of Buyer Data, and providing this information to the Supplier upon the Supplier's request to support the Supplier's completion of the Exit Plan. o The transfer of the Buyer's owned Project Specific IPR items (MOJ Developed Products) and other Buyer owned customisations, configurations, and databases to the Buyer and/or a Replacement Supplier. o The testing and assurance strategy for exported Buyer Data. The Buyer is responsible for defining the standards for the exportation and migration of Buyer Data and providing this information to the Supplier upon the Supplier's request to support the Supplier's completion of the Exit Plan. o Any potential costs to the Buyer associated with the above services. • The procedure for fully decommissioning of the Supplier's hardware equipment at each prison site and the removal of any leased hardware equipment from the Supplier at the prison sites. • Roles and responsibilities for the Supplier Staff and/ or the Supplier's Subcontractor Staff, and the Buyer Staff in completing these decommissioning activities of the Supplier's hardware and removal of Supplier leased hardware from the Buyer's prison sites. • Total costs for decommissioning the Supplier's hardware equipment at each prison site and the removal of any leased hardware equipment from the Supplier at the prison sites, including but not limited to: o Time and Materials costs for the Supplier staff to complete these activities at each prison site (all costs will align to the SFIA Day Rate charges included in Schedule 5 of this Call-Off Contract). o Travel and Subsistence costs for the Supplier staff to complete these activities at each prison site (all costs will align to the Ministry of Justice's Travel and Subsistence policy and all charges in Schedule 5 of this Call-Off Contract.)

	• Total costs for decommissioning the Supplier's software within the Supplier's hardware at all prisons in scope of this Call-Off Contract, including but not limited to:
	  ○ Time and Materials costs for the Supplier staff to complete these activities at each prison site (all costs will align to the SFIA Day Rate charges included in Schedule 5 of this Call-Off Contract).
	  ○ Travel and Subsistence costs for the Supplier staff to complete these activities at each prison site (all costs will align to the Ministry of Justice's Travel and Subsistence policy and all charges in Schedule 5 of this Call-Off Contract.)
	• The destruction of confidential information associated with off-boarded sites including permanent erasure of and data stored on decommissioned equipment. The Supplier will provide a data destruction certificate to the Buyer to confirm that this has been completed.
	
	More broadly, as per the terms and conditions of this G-Cloud 12 Call-Off Contract, the Exit Plan shall also include (but shall not be limited to):
	• Provisions relating to Contract Exit for the supply by the Supplier of all such reasonable assistance as the Buyer shall require enabling the Buyer or the Buyer's third-party Suppliers to provide the Services;
	• The management structure to be employed during both transfer and cessation of the Services during Contract Exit;
	• A detailed description of how the Services will transfer to the Buyer and/or the Replacement Supplier(s), including details of the processes, documentation, data transfer, systems migration, security and the segregation of the Buyer's technology components from any technology components operated by the Supplier or its Sub-contractors (where applicable);
	• Procedures to address each of the issues set out in this Exit Management plan to facilitate the transition of the Services from the Supplier to the Buyer and/or the Replacement Supplier(s) with the aim of ensuring that there is no disruption to or degradation of the Services during the Exit Management Period;
	• Detailed descriptions of where Sub-contractors support the delivery of the Services and how these

	Sub-contractors may be impacted by or required to support the Contract Exit services; • The plan for return and destruction of the Buyer's Personal data as held by the Supplier for this Call-Off Contract. The Buyer is responsible for providing this information to the Supplier. The Buyer will provide the Supplier instructions the plan for the return and destruction of Buyer personal data and the responsibilities of both Parties within 90 days of the Call-Off Contract Start Date. This will include confirmation of the date of the Supplier's destruction of the Buyer's data; • Any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition. To support these activities, both the Buyer and the Supplier will appoint an Exit Manager and provide written notification of such appointment to the other Party within three (3) months of the Call-Off Contract Start Date. The Supplier's Exit Manager will be responsible for ensuring that the Supplier and its employees, agents and Sub-contractors comply with this Exit Management document. The Supplier will ensure that its Exit Manager has the requisite authority to arrange any resources of the Supplier as are reasonably necessary to enable the Supplier to comply with the requirements set out in this Exit Management document. The Buyer's Exit Manager will be responsible for managing the exit plan arrangements with the Supplier, upon receiving the Contract Exit Plan from the Supplier within three (3) months of the Call-Off Contract Start Date. The Buyer is responsible for reviewing this Exit Plan provided by the Supplier, confirming if adjustments are required for the Exit Plan and finalising the Exit Plan arrangements with the Supplier. The Buyer's Exit Manager may request additional support from the Buyer's Staff, and the Buyer's third-party Supplier Staff, to support the finalisation the Exit Plan arrangements with the Supplier. The Buyer's Exit Manager is responsible for clearly defining to the Supplier the exit management arrangements for data migration and transfer to the Buyer at Contract Exit. This will be led by the Buyer's Exit Manager upon receipt of the Supplier's Exit Plan and to be formalised by the Supplier and the Buyer in the Exit Plan.

	The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the Contract Exit Plan on a monthly basis, and all matters connected with the exit management requirements and the Supplier's and the Buyer's, and the Supplier's Subcontractors, compliance with the Exit Plan.
Collaboration agreement	The Supplier may be required to enter into Collaboration Agreement during this Call Off Contract period. The Supplier shall work proactively, collaboratively and in good faith with the Buyers Contractors, Prison Staff, the prisons' Single Point of Contact (SPOC), and HMPPS Digital.
Limit on Parties' liability	[REDACTED]
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 60 consecutive days.
Audit	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits. This also includes clauses 7.4 to 7.13 of the 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 Subcontractors' costs) and any variations to them, including proposed variations 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, Government Internal Audit Agency, the Comptroller 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. The Buyers' users in HMPPS Digital will have access to the Supplier's real-time audit information. The Buyer may have access to the Supplier's audit data on a quarterly basis. This includes financial information, service running time, maintenance, security issues and patching done to address those issues. The Buyer may define how long this audit information is stored for. The Supplier will store this audit information for at least 12 months.
Buyer's responsibilities	This is an overview of Buyer responsibilities throughout this Call-off Contract. Buyer responsibilities for specific prison types are detailed in Schedule 1 below. The Buyer is responsible for the following requirements under this Call-Off Contract: 1. Selecting establishments for roll-out of in-cell technology services, authorise plans for implementation of Unilink services and timing. This will be specified by the In-Cell Technology Deployment Plan. Roll-out will occur in three groups: a. Group A consists of [REDACTED]. Rollout will be complete for this group by Summer 2021. b. Group B consists of [REDACTED], with deployment occurring Mid-to-Late 2021. c. Group C consists of [REDACTED] with deployment planned for late 2021 and early 2022 2. Select work streams and work with Unilink to define each, including managing live services, upgrading sites, and supporting the roll-out for In-Cell Technology. 3. Each site will nominate a SPOC (Site Point of Contact) who will be the main point of contact for the Unilink Project Manager in HMPPS Digital and Unilink's engineers for this project. 4. Ensuring that Unilink engineers will have full access to all relevant work areas at each site when required to perform installation, configuration or maintenance on behalf of the Buyer and/ or perform a site survey. The Buyer will be responsible for ensuring that each site required to be attended by the Unilink engineer will have a sufficient number of escorts is available for

each engineer; confirming the designated areas where the engineers will need to attend, and for managing the allocated dates/ times when the Unilink engineer will attend the relevant site. Unilink will coordinate with the MoJ allocated project Manager and each site individually, so that the implementation can proceed according to the planned delivery at each site.

5. Each site will ensure any required site work as identified at meetings: GAP Analysis, Site Survey and meetings with HMPPS Digital Project Manager or designated service lead, and establishment site designated Single Point of Contact, will be completed prior top agreed installation date.
6. The Buyer's service desk and HMPPS Digital team are responsible for managing and maintaining the Cloud platform where software for Digital Prisons under this Call-Off Contract will store their data.

Exit Arrangements

As per the Offboarding requirements of this Call-Off Contract order Form, the Buyer's Exit Manager will be responsible for:

7. managing the exit plan arrangements with the Supplier, upon receiving the Contract Exit Plan from the Supplier within three (3) months of the Call-Off Contract Start Date. The Buyer is responsible for reviewing this Exit Plan provided by the Supplier, confirming if adjustments are required for the Exit Plan and finalising the Exit Plan arrangements with the Supplier. The Buyer's Exit Manager may request additional support from the Buyer's Staff, and the Buyer's third-party Supplier Staff, to support the finalisation the Exit Plan arrangements with the Supplier.
8. The Buyer's Exit Manager is responsible for clearly defining to the Supplier the exit management arrangements for data migration and transfer to the Buyer at Contract Exit. This will be led by the Buyer's Exit Manager upon receipt of the Supplier's Exit Plan and to be formalised by the Supplier and the Buyer in the Exit Plan.
9. Clearly defining to the Supplier the exit management arrangements for data migration and transfer to the Buyer at Contract Exit, upon receipt of the Supplier's Exit Plan and to be formalised by the Supplier and the Buyer in the Exit Plan.
10. Clearly defining to the Supplier the plan for the return and destruction of Buyer personal data and the

	responsibilities of both Parties. This will be provided within 90 days of the Call-Off Contract Start Date.
Buyer's equipment	This is an overview of Buyer equipment to be utilised across the 27 prisons throughout this Call-off Contract. Buyer equipment to be utilised for specific prison types are detailed in Schedule 1 below. The Buyer's equipment to be provided for use with this Call-Off Contract includes: • Terminals, end-user devices and printers as required. These devices can be specified by the Supplier or provided by the Supplier at additional charge. • Provision of Network connectivity to connect cloud services as required for security accreditation • Cabling of Kiosks & WiFi access points to the network connection

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners who will support in providing the following services under this Call-Off Contract: [REDACTED]

Call-Off Contract charges and payment

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

Payment method	The payment method for this Call-Off Contract is BACS.
Payment profile	The payment profile for this Call-Off Contract is 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
	• Name of Establishment(s) where services were delivered to
	• Unit measurements for software and hardware services, as per the Call-Off Contract period
	• Details of charges for the invoice period, including:
	  ○ Which Support Services and Maintenance services were provided for the invoicing period
	  ○ The charges for each of these Support Services and Maintenance Services for the invoiced period.
	  ○ SFIA Rates for any Capped Time and Material Charges for services delivered against the SFIA rate card for this Call-Off Contract
	  ○ A breakdown of the fixed monthly charges for each of these services charges for these invoices, as per this Order Form and Schedule 2 of this Call-Off Contract.

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 £3,520,000.00.
Call-Off Contract charges	[REDACTED]

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. Milestones for the In-Cell Technology Programme rollout are: • Successful implementation of the web client on MoJ devices, ensuring that a prisoner can access Unilink services on an MoJ device. • Successful completion of an ITHC CHECK, including collaboration in developing the scope and agreeing any remedial actions needed to complete the test. • Support model and plan for monthly security patching agreed. Rollout will be completed in three stages, at the following times during this Call-Off Contract term (Quarterly periods in this timetable are aligned to calendar year periods, rather than Financial Year calendar periods): Completed by end of Quarter 2 2021 (June 2021): [REDACTED] Completed by end of Quarter 4 2021 (December 2021): [REDACTED] Completed by mid-Quarter 1 2022 (February 2022): [REDACTED] This Call-Off Contract will include BAU of the existing 15 prisons plus the implementation plan and milestones to be developed for each of the additional 12 establishments as directed by the In-Cell Programme team. The Call-Off contract also incorporates the exit and offboarding plans.
Guarantee	N/A
Warranties, representations	N/A
Supplemental requirements in addition to the Call-Off terms	N/A

Alternative clauses	N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms	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: Overview of Services across all Prisons

The Services to be delivered by the Supplier to the Buyer over the term of this Call-Off Contract will be in line with the Supplier's Service Offering 843642414370275, and as per the below. Schedule 1 will outline all services that shall be delivered within all 27 prisons in scope of this Call-Off Contract.

These services are to be delivered to the following prisons.

Digital Prisons: Prisons with Prisoner self-service and integrated with PNomis via real-time API. On-premise or in the MOJ Azure cloud both of which are managed by the Buyer. These prisons have biometric touch screen kiosks available on wings and common areas of each prison.

In-cell Digital Prisons: Prisoners able to access Prisoner Self-service via in cell-devices.

Standard prisons: Standalone on-premise software with no real-time interface to PNomis.

Some services under this Call-off Contract are specific to the type of prisons. Services specific to Digital Prisons, and services specific to In-Cell Digital prisons, can be found in Schedule 2 of this Call-Off Contract. Services specific to Standard prisons can be found in Schedule 3 of this Call-Off Contract.

[REDACTED]

The In-Cell Technology Plan has defined when all prisons listed as in-cell Digital prisons will be fitted with in-cell technology. The prisons will be fitted with in-cell technology as part of three groups. Rollout will be completed in three stages, at the following times during this Call-Off Contract term (Quarterly periods in this timetable are aligned to calendar year periods, rather than Financial Year calendar periods):

1. Completed by end of Quarter 2 2021 (June 2021): [REDACTED]
2. Completed by end of Quarter 4 2021 (December 2021): [REDACTED]
3. Completed by mid-Quarter 1 2022 (February 2022): [REDACTED]

Software Modules for all Prisons

The software modules listed below are provided by the Supplier for use by the Buyer throughout this Call-Off Contract for all service users. All these software modules as outlined in this Call-Off Contract are provided by the Supplier to the Buyer for use under this Call-Off Contract as per the terms of Clause 11 - Intellectual Property Rights of this G-Cloud Call-Off Contract Terms and Conditions. The software modules lists are split between Prisoner facing modules used by offenders within prisons in scope of this Call-Off Contract, and staff facing modules used by HMPPS Staff within prisons in scope of this Call-Off Contract.

All software modules for Prisoner Facing modules are used within all Standard Prisons, and all Digital Prisons. In-Cell Technology Programme will only use a selection of modules as identified in the In-Cell Technology Programme MVP document. In-Cell Technology prisons will not use the following software modules at any point during this Call-Off Contract:

- FAQs
- Noticeboard

At any time during the Call-off Contract, if the Buyer chooses to end the use of any of the Supplier's software modules provided as part of this Call-Off Contract, for Prisoners or for Staff, at one or more of the Buyer's prison sites included within this Call-Off Contract, a designated representative on behalf of the Buyer from HMPPS Digital team will notify the Supplier of the intention to no longer utilise one or more of the Supplier's software modules at one or more of the Buyer's prison site(s). The Buyer's designated representative from HMPPS Digital will provide the Supplier with at least 15 working days written notice (an email is accepted as in writing) of the software module(s) to no longer be used at the Buyer's prison site(s).

Prisoner Facing Modules

Prisoner Module Features

The Supplier's self-service kiosks modules are provided in the following languages for all Prisoners within the prisons in scope of this Call-Off Contract:

Albanian, Arabic, Bengali, Dutch, English, Farsi, French, German, Latvian, Lithuanian, Mandarin, Polish, Punjabi, Romanian, Slovak, Spanish, Tamil, Urdu, Vietnamese and Welsh.

Additional languages can be added on request at an additional cost per language.

Prisoner Facing Modules List

Provides account balance and account summary with detailed transactions view. Account Balance ties into the backend Finance module, which records incoming transactions from Prisoner's pay, incoming funds or savings and outgoing transactions from Canteen shopping, Pin Phone Top-up or special request payments.

Items for sale are clearly displayed with pictures to assist Prisoners with reading difficulties, with clearly indicated out of stock items. Provides controls on spend restrictions and sale item restrictions. It enables real time update of account balances, can be linked to Establishment Shop to assist with inventory and stock control.

Prisoners can purchase pin phone top-up from the kiosk, which are credited to the phone provider and updated in real time. They can view their call history, phone balance, their approved numbers etc.

Enables Prisoners to pre-order their meals from menus displayed clearly on screen (can include pictures). Meals can also be assigned health and nutrition symbols, i.e. 5-a- day, as well as special dietary markings. Prisoner menu choices are immediately transmitted to kitchen staff, removing the requirement for officers to collate paper-based selections.

Tied in with the NForce CMS Scheduling and Apps modules, Timetable displays the prisoners planned activities for up to two weeks in advance. It encourages prisoners to be responsible for managing their own time, reducing the demand on officers'.

Read only notices or information to prisoners posted by the establishment.
The notice-board modules will not be employed in in-cell technology prisons.

Prisoners can book their social visits on the kiosk, through clear, user-friendly on-screen instructions. The applicable visits entitlements, approved visitors and available dates/time slots are clearly displayed. Visits booking is a fully automated process, only available visit slots are shown to the prisoner.

Prisoners can make standard, pre-defined applications (requests), choosing from a drop-down list of available requests. The application is sent to the corresponding department for processing and response and their status and responses are displayed to the prisoner on the self-service device.
Some requested activities are automatically approved, scheduled and displayed in the prisoner's timetable. Appointments can be requested and cancelled directly from the self-service device.

Features searchable information - questions prisoners most frequently ask, and the establishment's standard responses. The questions and answers are grouped by common categories for ease of use.
The FAQ module will not be employed in-cell technology prisons.

Displays prisoners key information pertinent to them: Case log and important info e.g. Earliest Date of Release, personal case officer etc. The prisoner is notified when the casework department has updated a field.

A variety of Surveys can be posted by the establishment to prisoners to complete, allowing answers in defined formats i.e." Yes/No", pick from drop-down lists, enter free text/comments etc.

Messaging displays internal messages from staff and external messages from approved contacts. Family & friends, or legal contacts, can use EMAP (Email a prisoner) service, to send messages to a prisoner, which can be either presented on any self-service platform, or alternatively printed out in the Ward and delivered to the cells manually.

Enables access to external content:

- Education Videos and Education Courses
- Behavioural courses- description/services
- Any other in future... music, videos, e-books

Staff Facing Modules

This section identifies the Staff Facing Modules available within this Call-Off Contract. However, not all modules will be available in each prison in scope of this Call-Off Contract. Upon request, the Buyer shall provide the Supplier information about deployment of Staff Facing Modules at each of the prisons in scope of this Call-Off Contract within 10 working days of this request being received.

CMS RECEPTION

A core module used to capture biometric and demographic details of prisoners. It is the 'hub' for prisoner Record management:

- Biometric/Photo enrolment, Smart card assigning, Badge and image printing
- Prisoner Property management, Checklists (custom Q&A), event-logs,
- Associations (links, families, lead, gangs) prisoner warnings and restrictions – drives work-flow

CMS RESIDENTIAL

Housing management – Manage prisoner activities, punishments and housing restrictions

- Electronic cell sharing risk assessment warns when potentially housing prisoners with medium/ high risk with other prisoners.
- Graphical view of prisoners housed on a wing
- Review diary and reporting of prisoner charges and punishments
- Cell card with prisoner photo

CMS VISITS BOOKING

Is a fully automated booking tool for social, legal and official visits, with configurable business and security rules.

This automated process shows only available visit slots, according to pre-defined rules and person restriction.

- Configurable prisoner and visitor warnings with associated business logic.
- Ability to ban or approve visitors and helps preventing inappropriate visits.
- Separates gang members automatically into different visit times.
- Enables identification of suspicious visit activity
- Includes online Booking engine for Legal Visitors, prisoner Self-Service visit booking function with automatic visitor notification by Email and SMS
- Fully searchable database with an integrated report writing tool.

CMS VISITOR MOVEMENTS

Encompasses all visitor types (social, legal, official) and enables biometric ID/security checks at required points:

- Biometric enrolment of visitors enables biometric scan at each access point, increasing security.
- Automatic flagging of unauthorised entry/exit and banned visitors.
- Integrates with barrier control to automate the visit movement process

CMS STAFF ACCESS

Biometric Staff system enables automatic recording of staff on-site and provides a record of any key skills (e.g. hostage negotiator, fire marshal, first aider etc.)

- Produces high quality ID cards
- Records allowed/prohibited items against individual staff members
- Interface to key/radio vending system and turnstiles to for access control.

CMS FINANCE

The processing of all prisoner's monies and transactions - automates payment processes. It integrates seamlessly with Shop and Phone to provide real-time account debit/credit.

- Integrated with CMS Scheduling and CMS Employment to streamline and automate prisoner pay
- Integration with Secure Payment Services provides electronic cash transfer from registered users to prisoners, reducing the cash handling requirements.

CMS SHOP

Front and back-office support for a variety of shopping experiences: face-to-face, bag-and-tag and/or Self-Service. It is fully integrated with CMS Finance, enabling rapid reconciliation and analysis of sales of goods to prisoners.

- Controls on spend and sale item restrictions.
- Includes stock management and assists with inventory and stock control.
- Support for cash, cashless or mixed payment types

CMS SCHEDULING

Sophisticated tool enables intelligent scheduling of all prisoner activities and events, following configurable rules and business logic.

- Activities are prioritized according to the applicable rules, even when more than one event is scheduled for the same time period.

- Allows the creation of Waiting lists based on requirements
- Attendance recording can automate associated pay.
- Prisoners can self-schedule certain activities automatically (e.g. Gym) using Self-Service functionality. This is displayed on the individual prisoner's timetable and sent to the relevant department (e.g. gym).

CMS MENUS

Used with self-service function, allows automated reporting on prisoner food selection, enabling kitchen staff to quickly and easily determine the meal requirements for each day, significantly reducing food wastage. Menus are loaded onto the system with health symbol keys and optional photos of the food items.

CMS NOTICEBOARD

Used with self-service function, publishes notices to prisoners for viewing on self-service devices. A notice can be sent to all prisoners or a selection of based on configurable criteria. The system also records when the Notice has been read, providing an auditable trail.

FREQUENTLY ASKED QUESTIONS (FAQ)

Used with self-service function, this module features questions prisoners most frequently ask, and the establishment's standard responses. The questions and answers are grouped by common categories that can be changed or refreshed at any point.

CMS APPLICATIONS/REQUESTS

Automated prisoner application system (requests) used with self-service function it enables the creation of request categories and application criteria to allow prisoners to make requests on self-service devices, e.g. appointments, submit applications, jobs, courses etc. The establishment has an audit trail of all applications; their status and their response time.

CMS CASEWORK

Used with self-service function to give prisoners key information pertinent to them: Case log and prisoner important info e.g. Earliest Date of Release, personal case officer etc. It allows staff to send a one-way message to a prisoner and enter contact log information.

CMS EDUCATION/ASSESSMENT MODULE

Provides effective monitoring of prisoner achievements, qualifications and allows the creation of custom assessments with setting targets.

- Qualifications can be assigned, awarded and tracked throughout the system. Pending qualifications can quickly and easily be monitored and updated.
- Integrates with scheduling - assessed individuals with targets set are scheduled onto activities to work towards those targets.
- Activities can be tied to qualifications and assessments so that success and retention statistics can be produced from the system.
- A "learner journey" screen provides the ability to quickly review an individual's activity history and progress against their targets.

CMS SURVEYS

Enables authorised users to create custom surveys that prisoners complete by using the self-service functionality. It allows staff to define each survey question and the format the answer will take, with an integrated reporting tool, enabling full analysis of survey results. Criteria logic enables surveys to be targeted to specific groups of prisoners.

CMS TRANSLATE

Allows staff to display self-service kiosk data items translated into multiple languages, for example meal menu items, canteen items, timetabled activities etc. Staff can export the existing English items for translation and then import translated items. CMS translate combined with multi-language Self-Service devices, enables effective communication with prisoners in the language of their choice.

CMS LIBRARY

A fully functional library system; using smart card or fingerprint technology books/items can be reserved, issued or returned to prisoners quickly and easily. Standard ISBN numbering along with internal numbering is used to catalogue items.

CMS HOUSEKEEPING

Housekeeping is a core module, required to enable system administrators to manage the entire NForce CMS system. Changes can be made to the base operation of the system without development costs making NForce CMS flexible and highly configurable system.

CMS SECURITY

Log and produce Security Incident Reports and Incident reports

CMS REPORTS

Comprehensive report writing tool: users create their own reports by setting the desired criteria/parameters, i.e. selecting the data fields that they want to appear on the report, specifying the sort order and selecting the report criteria.

CMS KIOSK

Contains all the prisoner facing self-service functionalities, enabling the desired configuration to be displayed on all or specific self-service device, i.e. choice of displayed modules.

Software Licensing

Unilink will grant to the MOJ a non-exclusive, non-transferable right to Use (and to permit the Authorised Users to Use) the Software and User Documentation during the Term solely for the MOJ's internal operations.

The MOJ will not:

- access all or any part of the Supplier's confidential information in order to build a product or service which competes with the Software;
- use the Software to provide services to third parties;

- license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Software available to any third party except the Authorised Users, or;
- attempt to obtain, or assist third parties in obtaining, access to the Software other than as provided under this Contract.

MOJ shall use reasonable endeavours to prevent any unauthorised access to, or use of, the Software and, in the event of any such unauthorised access or use, promptly notify the Supplier.

The Supplier will remove any user visible prompts for licence key renewals on users' desktops and substitute these with notifications to designated HMPPS Digital Project Manager staff on behalf of the Buyer. If required, the Buyer will provide the names and contact work email addresses for the HMPPS Digital Project Manager staff to the Supplier.

Software releases

MOJ will receive new release of software free of charge and typically once every three-six months. These releases will be packaged to an agreed specification with product support group ready for deployment/test. New releases will also include pertinent documentation covering the new release and its functionality/configuration as appropriate.

Upgrades will usually be via automation through supplied scripts from the supplier where possible, in certain circumstances updates/patches may be installed manually via remote access supplied by the Authority or Unilink. Updates and patches will typically be carried out in the identified maintenance windows agreed with the MOJ and Product teams.

Updates and Modifications:

Requests for Software updates and Product functionality modifications shall be submitted by MOJ through an agreed process via the HMPPS Digital Product Manager and receive approval from the Digital Prisoner Transactional Services Owner before any changes are submitted.

Any removal/modification of existing functionality by the Supplier must be communicated to the MOJ product team six months beforehand in sufficient detail to allow for impacting by MOJ. This would also cover API connectivity/ functionality.

Development

During this Call-Off Contract, the Buyer may request the Supplier to perform development work on behalf of the Buyer. This may include:

1. Development of API(s) to other MOJ systems or services, including enablement of interoperability between Unilink and other services via API
2. Development of communications with the authentication layer
3. Development of communications with the landing page and log in screen
4. Exploration of, and development related activity to support, look and feel / branding work streams
5. Two-way exchange of information with other HMG IT systems.
6. Conform of the Architectural and Data Principles of Justice

Where the Buyer has a requirement for development work during this Call-Off Contract, the Buyer will make the Supplier aware of these additional service requirements at least 30 days in advance of this requirement and request the Supplier provide a specific quote for delivering this work.

The Supplier will then share this specific quote for these additional services with the Buyer. All development work charges will align with the Call-Off Charges as provided under this Call-Off Contract Order Form and Schedule 5, and all developer charges will align to the Developer SFIA Level 6 Day Rates as outlined in Schedule 5. The Buyer will review this quote and agree any necessary work with the Supplier under a Statement of Work for this work. The Buyer and the Supplier will use the template included in Schedule 8 of this Call-Off Contract. Only once approval in the form of a Statement of Work detailing these changes has been signed off by both Parties, may this work be undertaken by the Supplier. For confirming these services have been delivered and may be paid via invoice, approval will first be provided by the HMPPS Digital Service Lead on behalf of the Buyer. These additional services charges will be paid by the Buyer within 30 days of receipt of a valid invoice.

Only once approval in the form of a written confirmation detailing these changes has been provided by a designated representative from HMPPS Digital or MOJ Commercial on behalf of the Buyer, and all works under this development work requirement are agreed by both Parties, may this work be undertaken by the Supplier. For confirming these services have been delivered and may be paid via invoice, approval will first be provided by the HMPPS Digital Service Lead on behalf of the Buyer. These additional services charges will be paid by the Buyer within 30 days of receipt of a valid invoice.

Data Back-Up

The Supplier shall work collaboratively with the Buyer and provide support, guidance and assistance, in relation to identifying what data needs to be backed up to ensure complete restoration of the service covering both front and backend services.

[REDACTED]

Information Assurance

The Supplier shall provide a secure software system which undergoes annual penetration (PEN) testing by an accredited CHECK organisation at the Supplier's own cost. Results of such testing will be made available to the Ministry of Justice on request.

In addition to the annual PEN testing the Supplier shall review any resulting vulnerability reports and invoke a remedial action plan for remedy as appropriate to the risk identified. Such action plans to be affected at Unilink's cost as part of their continuing product support. The Supplier will make the Buyer aware of any risks identified as part of this PEN testing which may impact the delivery of services for this Call-Off Contract or impact the integrity and protection of the Buyer's data within 2 hours of identifying a significant risk to the system, and shall take all appropriate actions to mitigate this risk. The Buyer shall maintain good communications with the Buyer's designated Point of Contact for this service, including the Buyer's HMPPS Digital Project Manager and HMPPS Digital IT and Cyber Security Lead, and provide regular updates (at least once every 4 hours per working day) of actions taken by the Supplier to mitigate this risk. The Supplier shall provide a remedial action plan for remedy as

appropriate to the risk identified within 5 working days of the risk being identified, to the Buyer for review. 5 working days for provision of the remedial action plan to the Buyer is a latest date for delivering this service, and the Supplier should provide this plan as soon as reasonably possible in advance of the 5 working days' deadline to the Buyer.

The Supplier shall co-operate with any PEN testing on MOJ Hosted implementations where Unilink software components/services are installed. The Buyer will notify the Supplier in good time of this Pen Testing on MOJ Hosted implementations where Unilink software components/services are installed.

Hardware Requirements

All hardware equipment under this Call-Off Contract will be provided via one of the following scenarios:

1. Hardware is leased from the Supplier by the Buyer for the purposes of delivering these services under this Call-Off Contract, for the duration of this Call-Off Contract.
2. Hardware is provided by the HMPPS establishment of behalf of the Buyer.
3. In-Cell Technology is provided by the HMPPS establishment by the Buyer.

For all hardware leased by the Buyer from the Supplier, the Supplier shall provide hardware maintenance support for each items of this equipment. Any hardware equipment provided as per the lease for this Call-Off Contract shall not be purchased by the Buyer at any stage during the Call-Off Contract, during any extension period, or after the Call-Off Contract End Date.

Replacement and/or repair of a faulty component, supplied by Unilink, is free of charge under warranty, except when fault, or damage is caused by the Buyer's or the Buyer's service users' negligent handling, or deliberate damage by the Buyer or the Buyer's service users. In the case of fault, damage or deliberate damage is caused by the Buyer or the Buyer's service users to the Supplier's hardware equipment leased by the Buyer under this Call-Off Contract, the maintenance and repairs costs will be chargeable to the Buyer by the Supplier. This is as defined in the hardware support table below.

Quantities for each of this hardware equipment used at each Establishment is different and should be confirmed with the Buyer's Single Point of Contact and HMPPS Digital Project Manager for each of the establishments.

Hardware Locations

A full system when implemented will typically cover and shall be agreed by the Parties.

***Inmate Reception*:** biometric enrolment (fingerprint scan, photo) and discharge of prisoners. Additional information is entered (keep apart markers, warnings etc.), to enable functionalities of CMS modules. The system assigns a unique PIN number which, combined with the fingerprint identification, enables the detainee to log on to the kiosk. Biometric data is also used to accurately identify the prisoner at various points in the prison (e.g. Shop, entry/exit to workshops etc.) providing additional security.

***Visitor Centre, Visits Hall, Gate, Vehicle Lock (depending on establishment layout)**:* biometric enrolment of social and legal visitors (number of locations depending on the layout). This is required to enable associating the visitors to a particular prisoner and to provide an accurate biometric ID

check, increasing the security and providing useful intelligence information. Additionally fingerprint readers are positioned at several checkpoints on the way into the actual visits hall (depending on the layout) to prevent any possibility of escape through the visits route.

Gate, Vehicle Lock: Biometric enrolment of official visitors, biometric entry/exit control through doors and/or turnstiles including staff access control with interfaces to key/radio cabinets (e.g. Traka) and turnstiles (e.g. Gunnebo).

Various Administration Offices*:* Security, Finance, Kitchen, Health, Stores, Gym, Chaplaincy, Industries/Education/Programmes etc. require workstations and optional Printers to allow staff access to the system and enable the administration of prisoner requests arising from the self-service functionalities.

House Blocks: **prisoner** self-service kiosks are usually positioned on the house blocks/wings and/or in communal areas to allow prisoners easy access. A PC workstation at the wing Staff Office is recommended to enable staff access to the system.

Work/Education Areas: potential additional kiosk access location. Recording attendance is automated by biometric check at entry/exit, which can be used to automate attendance payments.

Hardware Support Table

Warranty period for all items	***12 months***	***Free replacement of faulty equipment (parts and labour), exceptions apply***
Standard Support (Post	***1 to 5 years***	***Items supported until their expected lifespan - as per table below***
Beyond Expected Lifespan	***Over 5 Years***	***Replacement recommended thereafter, supported until Beyond Economic Repair - BER***
Limited Support	***Over 10 Years***	***Some replacement may not be possible unless the whole system is refreshed***

Excluding deliberate damage, or damage caused by inappropriate handling. Such replacement is chargeable - parts and labour

ITEM	Expected Lifespan	Repair Method	What is supported during expected length of life period
Server	5 Years	onsite repair	HDD replacement on site free for the first 12 months; chargeable thereafter
NAS drive	3 – 5 Years	onsite repair	HDD replacement on site free for the first 12 months; chargeable thereafter
Server UPS	3 – 5 Years	onsite replacement	Return To Base to Unilink. On site batteries replacement - chargeable Consumables
PCs - Workstation	3 – 5 Years	onsite repair	HDD replacement on site free for the first 12 months; chargeable thereafter
UPS	3 – 5 Years	onsite replacement	Return To Base to Unilink. On site batteries replacement - chargeable Consumables
Camera	5 Years	RTB Unilink	Free replacement Return To Base to Unilink for repair
USB adapter	3 – 5 Years	RTB Unilink	Free replacement, chargeable for deliberate damage
Badge printers	3 – 5 Years	RTB Unilink	Swap out replacement; Return To Base to Unilink for repair – chargeable if Buyer damaged or BER
Other printers	3 – 5 Years	onsite repair	Onsite repair or replacement if not possible; chargeable if damaged by the Buyer, or BER
Fingerprint readers	3 – 5 Years	RTB Unilink	Return To Base to Unilink to be repaired, Chargeable If damaged by the Buyer
KIOSKS			

Whole kiosk	5 Years	RTB Acante *	Free replacement/ repair during warranty – excluding deliberate damage, or negligent handling.
Kiosk Screens	3 – 5 Years	onsite replacement	On-site swap out - free repair for the first 12 months - chargeable thereafter
Kiosk Fingerprint reader	3 – 5 Years	onsite replacement	Return To Base to Unilink to be repaired, loan replacement provided, Chargeable If damaged by the Buyer.
Kiosk UPS	3 Years	onsite replacement	Return To Base to Unilink. On site batteries replacement - chargeable Consumables
NETWORK			
Switches	3 – 5 Years	onsite replacement	Onsite replacement, chargeable if fault is caused by damage by the Buyer.

* Acante - kiosk Manufacturer – part of the Group.

Schedule 2 – Digital Prisons

The following prisons are identified as Digital Prisons, or will become Digital Prisons, over the duration of the Call-Off Contract period (between 16th April 2021 – 15th April 2022).

[REDACTED]

These prisons provide self-service kiosks on Wings only, with all software installed in the MOJ Azure cloud, which is managed by the Buyer.

[REDACTED] will be included in this Call-Off Contract within the Buyer's cloud solution

Hardware Provisions

With the exception of [REDACTED] , all hardware equipment is leased from the Supplier by the Buyer for the purposes of delivering these services under this Call-Off Contract, for the duration of this Call-Off Contract. The Supplier shall provide hardware maintenance support for each items of this equipment. Any hardware equipment provided as per the lease for this Call-Off Contract shall not be purchased by the Buyer at any stage during the Call-Off Contract, during any extension period, or after the Call-Off Contract End Date.

The Supplier shall provide hardware maintenance support for each items of this equipment listed in the assets section listed in Schedule 9 of this Call-Off Contract.

Quantities for each of this hardware equipment used at each Establishment is different and should be confirmed with the Buyer's Single Point of Contact and HMPPS Digital Project Manager for each of the establishments.

Software Support and Maintenance

Live Service Support

1. License to use CMS self-service new release at no additional charge during the contracted period.
2. Software patches, new releases and additional modules. New releases are typically published every 3 to 6 months. MOJ will be notified of the content of these releases when the release content has been finalised by Unilink.
3. Comprehensive Unilink supplied hardware and software support and maintenance.
4. Unlimited number of calls to the support line, including assistance over the phone
5. Hardware 'swap-out' maintenance of all equipment supplier by Supplier as part of the CMS deployment
6. Monthly review of the overall performance of the service conducted by the Supplier and shared with the Buyer, including incidents, changes, and performance of the service.
7. Annual Audit of the Supplier's IT Health Check conducted by the Supplier and provided to the Buyer to ensure that the Services are being appropriately maintained.

8. Additional related service e.g. postcode look up SMS messaging including support and management of the Online Legal Services Visits Booking process and additional web-based services such as links to emails a prisoner, video-visit and payment solutions.
9. User group subscriptions
10. Escrow services to make the software code available in case of disaster recovery or financial distress
11. Support any hardware or software associated with linking to Traka

Digital Prisons Support Model
The Supplier shall provide hardware maintenance support for each items of this equipment listed in the assets section in Schedule 9 below.

Quantities for each of this hardware equipment used at each Establishment is different and should be confirmed with the Buyer's Single Point of Contact and HMPPS Digital Project Manager for each of the establishments.

Digital Prisons Support and Maintenance

The service level and availability criteria required for this Call-Off Contract are;

Service Availability

Normal overall system service levels are measures at the point of use are 98% monthly in normal supported hours. In event that higher service levels are required up to 99.9% availability can be achieved by the use of duplexed high availability systems with no single point of failure. This is measured at overall system level i.e. failure of the main components or the application not the failure of an individual end user device.

Availability: Services will be available over at least 98% of the working day measured monthly excluding planned downtime subject to the networking and cloud infrastructure being available.

Service Day. Such applications are available 24X7x365 days per annum, a service day is between 08.00 and 17.00 Monday to Friday.

Outside Service Desk Hours. The fix times occur within manned Service Desk hours. At weekends and Bank Holidays the Supplier will attempt to meet the Service levels but will not guarantee fix times. However, critical components of the system, such as servers, are supported 24x7x365.

Down time: Any planned downtime *of the system will not exceed two hours during any "Service Day". The frequency of this downtime will not exceed two occurrences in any three month period unless specifically requested or agreed with the Buyer. The Buyer will be given at least seven days' notice of planned downtime within the service day and shall align to the Buyers Change control processes.*

Incident management

ServiceNow is the chosen tooling (note ServiceNow tooling may change during the course of this Call off Agreement). For all sites and Services, the MoJ service desk will "catch and dispatch" incidents. The Supplier will be set up as a resolver group in the ServiceNow toolset, the Supplier will be responsible for updating the incidents/ cases as they are progressed. Where the Supplier identifies as incident, the Supplier will communicate this to the service desk within 1 hour of identification if an incident, or immediately is severe/ urgent.

If it becomes apparent during the investigation of the incident that the Severity Level assigned to it appears incorrect, the Supplier will discuss the matter with MoJ and agree a new Severity Level in accordance with the agree Service level detailed in the tables below.

Service Levels

The following service levels shall apply:

Measurement	Definition
Severity 1 Fix or Workaround -Service level	Critical Business Operation down. Total loss of service or functionality impacts the Buyer's ability to operate its business. Examples: • Critical Systems/ Service Down • Whole site down • Whole estate down
Severity 2 Fix or Workaround -Service level	Significant portion of business operation down. Partial system/ critical/ core services are down impacting the Buyer's ability to operate its business. Examples: • Partial loss of service or functionality across the estate • Multiple users affected
Severity 3 Fix or Workaround -Service level	A unit or component failure which does not have a significant impact on the Buyer's ability to operate its business. Examples: • Partial loss of service or functionality • Individual user affected • No alternative available
Severity 4 Fix or Workaround -Service level	A minor disruption to service – User(s) can continue to work with majority of function Applies to unsupported or unlisted products. Examples: • Minor software bugs • Individual user has problems accessing a non-critical function • Alternative available
Severity 5 Fix or Workaround -Service level	A minor disruption to service – User(s) can continue to work with majority of function Applies to unsupported or unlisted products. Examples: • Minor software bugs • Individual user has problems accessing a non-critical function • Alternative available

Incident Escalation

The Supplier shall have effective and robust escalation procedures in place. In “critical situation” the Supplier’s MD in consultation with Technical Consultants will convene to reach an acceptable resolution. This will be agreed by the Parties.

Hot Fixes for Severity 1 incidents.

Incident Response Service Level – Software

Software SLA with remote access

Severity Level	System Impact/ Resolution
1	Resolve 95% of incidents within 2 hours for remote resolution or 4 hours if onsite presence required. 8 hours at all contracted sites. Service Hours (business day) excel Bank Holidays
2	Resolve 95% of incidents within 4 hours for remote resolution or 8 hours if onsite presence required. 8 hours at all contracted sites. Service Hours (business day) excel Bank Holidays
3	Resolve 95% of incidents within 1 business day if remote, 2 business days if onsite presence is required. Service Hours (business day) excel Bank Holidays
4	Resolve 95% of incidents within 3 business days, if remote, 5 business days if onsite presence is required. Service Hours (business day) excel Bank Holidays
5	Resolve 95% of incidents within 15 business days. Service Hours (business day) excel Bank Holidays

Hardware SLA

For all hardware support calls, initial response from a System expert will be within 2 hours (1 hour for High severity calls), from incident being raised.

Item Category	Initial Response	Feedback frequency	Resolution/ Fix Process
Workstations	Within 2 hours	8 hours if no status change/ fix	Workstation swap-out next business day
Kiosks	Within 2 hours	8 hours if no status change/ fix	Engineer onsite for repair/ replacement next business day
Networking	Within 2 hours	8 hours if no status change/ fix	Engineer onsite for repair/ replacement next business day
Peripheral Devices	Within 2 hours	8 hours if no status change/ fix	Item swap-out next business day

Hot Fixes for Severity 1 incidents. **Other support**

- Assistance in the testing and rectification of defects and deployment
- Investigation and resolution activities
- Work with resolver groups (i.e. MoJ development teams or other suppliers)
- Database support, consultancy, patching and management.
- Deployment, migration and transition of services.
- Enablement of interoperability between Unilink and other services via API’s
- Database Administration (Orchestrate on-going performance & scalability).

This work shall be performed in accordance with the GDS Digital Service Standard and Technology Code of Practise.

Performance Reporting

- Attendance at MoJ Checkpoint Meetings when required.
- Provision of monthly status reports, with a follow-up service review if necessary.

In addition to the above services the following support services will be required to be available to be called upon as required:

Schedule 3 – In-Cell Technology Prisons

The following prisons are identified as Digital In-Cell Prisons, or will become Digital In-Cell Prisons, over the over the duration of the Call-Off Contract period (between 16th April 2021 – 15th April 2022).

[REDACTED]

These prisons have biometric touch screen kiosks available on wings and common areas of each prison.

Onboarding Requirements – In-Cell Technology Prisons

The Supplier shall define and agree with the Buyer the implementation plan (milestone activities, meetings, logging issues etc.) and required documentation for each onboarding plan for Unilink's kiosks and in-cell technology hardware and software services each of the prison sites that are in scope of this Call-Off Contract. The Supplier will provide these implementation plans to the Buyer, and the Buyer will review and provide feedback within 10 working days of receipt. The supplier will work collaboratively with the Buyer or the Buyer's third-party suppliers in the agreement of the implementation plan and subsequent delivery of the in-cell solution.

The implementation plan shall include:

1. functional requirements brief;
2. Projects design - system architecture, including hardware specs & quantities;
3. Project plan with milestones (summarising project implementation phases);
4. Checklists, delivery records, and sign-off;
5. Hardware configuration and testing;
6. Integrated system testing - software and hardware at all locations;
7. Documented equipment's locations and serial numbers;
8. Training – records, materials and delivery;
9. Commissioning/ installation report and handover;
10. post-handover assistance to provide hands in help and expertise.

Testing

1. The Supplier shall work with HMPPS Digital to support and deliver acceptance testing.
2. Acceptance tests will include a range of functions including staff and self-service functionality, integration of the system with non-Unilink components and networking as defined by the Products team. The precise tests to be carried out will be agreed between the Supplier and the Product Teams and documented prior to any implementation.
3. Test scripts, outcomes and resolution to be agreed between Buyer and Supplier.
4. The Supplier shall work with the Buyer in issue management, including any regular sessions to agree issues, priorities and closure of issues found during testing.
5. The acceptance test agreements should address: test criteria, duration of test period, response time to issues that arise, the circumstances in which the system may be rejected, dispute resolution, level of resource required for testing on both buyer and seller's side, and identification of suitably qualified testers.
   In any circumstances that the Suppliers CMS product cannot be accepted into service by MoJ and is not live in that establishment then MoJ will not be charged by the Supplier for any services for that establishment.

In-Cell Testing and Training

The Supplier is to work collaboratively with the Buyer and any third-party suppliers in the design, development and delivery of the test and training environments. The Supplier will be required to make their software modules available in the testing and training environments that the Buyer is creating.

HMPPS Digital on behalf of the Buyer will provide information to the Supplier to facilitate the Buyer's requirement for the Supplier's software modules to be available in the Buyer's testing and training environments. The Buyer will give the Supplier reasonable notice of this requirement, and the Supplier must provide written confirmation of the intention to proceed with this. Only once the Supplier has provided written notification to the Buyer (an email is accepted as in writing) may the Buyer use the Supplier's software modules available in the Buyer's testing and training environments. The Buyer will ensure that in using the Supplier's software modules information in the testing and training environments, the Buyer will not infringe the Supplier's rights as per Clause 11: Intellectual Property Rights of this Call-Off Contract terms and conditions.

Data Back-Up

The Supplier shall work collaboratively with the Buyer and provide support, guidance and assistance, in relation to identifying what data needs to be backed up to ensure complete restoration of the service covering both front and backend services.

Any back up in the cloud will be managed HMPPS and will include all data held in the CMS.

Hardware provision

Typical hardware provision for in-cell technology prisons is:

[REDACTED]
Actual hardware required for each site will be confirmed during the site survey.

Support and Maintenance

The service level and availability criteria required for this Call-Off Contract are those listed in Schedule 2.

Schedule 4 – Standard Prisons

Standard Prisons

The following prisons are identified as Standard service prisons, which provide a different support model to the Digital and In-Cell Technology prisons outlined in this Call-Off Contract:

[REDACTED]

These prisons provide self-service Kiosks on Wings and use software which is installed on-premise. If any of these prisons will become a Digital Prison, HMPPS Digital's Service Lead on behalf of the Buyer will provide reasonable due notice to the Supplier of changes to scope of one of these/ multiple Prisons (at least 30 days). Any standard prison may only be transitioned to a Digital Prison, with the provision of services as outlined above in Schedule 2, upon signature of a Contract Change Notice.

Where the Buyer has a requirement to transition from a Standard Prison into a Digital Prison, the Buyer will make the Supplier aware of these additional service requirements at least 30 days in advance of this requirement. The Supplier will then share this specific quote for these additional services with the Buyer. All additional services charges will align with the Call-Off Charges as provided under this Call-Off Contract Order Form and Schedule 2. The Buyer will review this quote and agree any necessary work with the Supplier under a new Contract Change Notice for this work. Only once approval in the form of a Contract Change Notice detailing these changes has been signed off by both Parties, may this work be undertaken by the Supplier. For confirming these services have been delivered and may be paid via invoice, approval will first be provided by the HMPPS Digital Service Lead on behalf of the Buyer. These additional services charges will be paid by the Buyer within 30 days of receipt of a valid invoice.

Hardware Provisions

Hardware Provisions for Standard Prisons are as the below. All hardware equipment is leased from the Supplier by the Buyer for the purposes of delivering these services under this Call-Off Contract, for the duration of this Call-Off Contract. The Supplier shall provide hardware maintenance support for each items of this equipment. Any hardware equipment provided as per the lease for this Call-Off Contract shall not be purchased by the Buyer at any stage during the Call-Off Contract, during any extension period, or after the Call-Off Contract End Date.

Quantities for each of this hardware equipment used at each Establishment is different and should be confirmed with the Buyer's Single Point of Contact and HMPPS Digital Project Manager for each of the establishments:

- Server
- Server UPS
- NAS Drive
- Monitors
- PC UPS's

- CBM's
- MSO's
- PCs
- Colour LJ Printers
- B& W LJ Printers
- Badge Printers
- PCs
- Kiosks

The full assets list for HMP Manchester is found in Schedule 9 of this Call-Off Contract.

Support and Maintenance – Standard Prisons

1. <u>Service Availability</u>

1.1.1 Normal overall system service levels measured at the point of use are 98% on a monthly basis in normal supported hours. In the event that higher service levels are required up to 99.9% availability can be achieved by the use of duplexed high availability systems with no single point of failure. This is measured at the overall system level i.e. failure of the main components or the application not the failure of an individual end user device.

1.1.2 Availability: Such services are available over at least 98% of the working day measured monthly excluding planned downtime.

1.1.3 Service Day: Although such applications are available 24x7x365 days per annum, a “Service Day” is between 8:00am and 5:00 pm Monday to Friday.

1.1.4 Outside Service Desk Hours: The fix times occur within manned Service Desk hours. At weekends and Bank Holidays Unilink will attempt to meet the Service levels but will not guarantee the fix times. However critical components of the system, such as servers, are normally supported 24x7x365.

1.1.5 Downtime: Any planned downtime of the system will not exceed two hours during any “Service Day”. The frequency of this downtime will not exceed two occurrences in any three-month period unless specifically requested or agreed with the Buyer. The Buyer will be given at least seven days’ notice of planned downtime within the service day.

1.1.6 Backups: It is the responsibility of the Buyer to ensure daily back-up of the data processed by the Software. Where a fault has occurred and recovery of data is necessary, the Software will be restored with the most recent backup combined with database logs. Unilink will not be responsible for any data loss caused by a failure of the Buyer’s processes.

1.1.7 An annual audit of the system operation will be carried out and any recommendations noted to the Buyer. The annual maintenance of the server hardware is the responsibility of the Buyer.

2. Incident Management

2.1.1 When the Buyer identifies an incident, they communicate it to the Unilink Service Desk and an appropriate Severity Level is agreed in accordance with the following descriptions:

Severity Level	System Impact
High	System down or a significant part of the system not functioning and no workaround
Medium	Part of system failing or important and impacting problem however workaround
Low	Minor issues, general usage questions or request for minor change. Low severity

2.2 Incident Escalation

2.2.1 Robust escalation procedures are in place to ensure that call progress is monitored and that the priorities of outstanding calls are regularly reviewed. Where necessary, call priorities will be escalated through referral to the Senior Management Team in line with internal Escalation Procedures.

2.2.2 Unilink employ a number of processes and procedures with regards to support monitoring. This is typically encapsulated by the Support Help Desk Application, which is designed and 'plugged in' to the Microsoft Outlook working environment.

2.2.3 Unilink Software has dedicated call management staff, which are part of the central Operations Team, whose role includes the continuous monitoring of the support call database and appropriate response times. This responsibility also includes chasing and liaising with the account managers and the technical consultants and developers in order to achieve central call updating and successful closure.

2.2.4 In "Critical Situations" further action will be determined by the MD in consultation with the Technical Consultant(s) to reach an acceptable resolution. This could involve a wide range of possible actions, which are too diverse to record here, for example: on-site support, third party activity, additional hardware etc.

2.2.5 At all stages the Buyer will be kept aware of the state of progress without having to contact Unilink Software.

2.3 Incident Response Service Level - Software

2.3.1 The majority of 'Software Support' service calls can be resolved over the phone or with remote access. Remote access gives authorised technical resource to logon and complete initial diagnosis, analysis and even remote fault rectification in many circumstances, or can allow a 'temporary' fix to be applied if applicable. Application faults/issues needing a software patch represent very few and rare occasions.

2.3.2 Problems/issues with Application software, operating system, central database, web server/services, 3rd party drivers and SDK's are assessed and resolved according to the Software SLA table.

Software SLA without remote access

Priority	Initial Response	Feedback frequency	Resolution/Fix Process
High	Within 1 hour	4 hours if no status change/fix	Patch emailed/sent or resolved on phone, or engineer
Medium	Within 2 hours	8 hours if no status change/fix	Patch emailed/sent or resolved on phone, or engineer
Low	Within 2 hours	On status change/fix	Next version release

2.4 **Incident Response Service Level - Hardware**

2.4.1 For all hardware support calls, initial response will be within 2 hours (1 hour for High severity calls) from the call received by Unilink.

2.4.2 Unilink's response and potential fix time service level for Hardware Support is assisted by the cooperation of the relevant Buyer site and the Buyer site's Single Point of Contact (SPOC), for the purposes understanding the scope and impact of the problem. '

Hardware SLA

Item Category	Initial	Feedback frequency	Resolution/Fix Process
Central Servers	Within 1 hour	1 hour if no status change/fix	6 hours onsite response to start resolution
Workstations	Within 2 hours	8 hour if no status change/fix	Workstation swap-out within 48 hours
Kiosks	Within 2 hours	8 hour if no status change/fix	Engineer onsite for repair/replacement within
Networking	Within 2 hours	8 hour if no status change/fix	Engineer onsite for repair/replacement next
Peripheral Devices*	Within 2 hours	8 hour if no status change/fix	Item swap-out within 48 hours
Gunnebo Speedstiles**	Within 2 hours	2 hour if no status change/fix	6 hours onsite response to start resolution

* Peripheral Devices: Fingerprint scanners, Card readers, Badge printers, other printers

** Gunnebo Speedstiles are contracted through Unilink and directly supported by Gunnebo

3. Software Updates, Latest Releases Patches and Fixes

3.1.1 Buyers can typically expect to receive one upgrade once a year. Upgrades to the Buyer's licensed software modules are free of charge and may include functional enhancements and/or an upgrade to the technical environment. In addition to the upgrade, interim (patch) releases may be issued to resolve faults.

3.1.2. Upgrades and patches will normally be installed during Unilink's normal working hours (excluding Public Holidays) provided remote support is available. Interim release support: After the release of a new version Unilink will continue to support the previous version for a maximum of 24 months, unless otherwise notified. Under special agreements between the Buyer and it may be possible to extend this support period.

4. Support of Third¯Party Software

4.1.1. Servers and PC's have 3rd Party operating software installed – Microsoft: Windows Server and Windows for PCs. Microsoft periodically discontinues licence sale and support for older versions, therefore these cannot be replaced or updated and are not compatible with newer versions.

4.1.2. For example: Microsoft Server 2003 has ended in 2010, Server 2008 ended in 2015 and Server 2012 end date is 10/2018 - when/if a server fails, the relevant licence for replacement is no longer available for purchase. In case of PCs –
Windows XP is not supported/updated since 2014 and is considered a security risk, Windows 7 was discontinued in 2015 and support is extended to 2020. If a site needs to replace an old PC, the new one cannot be configured with the old
settings, hence it will not work.

4.1.3. Unilink will alert the site in case any of the operating systems in due to be discontinued that will affect the system supportability. Any installation that is over 7 years old, will require a system refresh to ensure that updates/upgrades can be applied.

5 Hardware Support and maintenance

5.1 Unilink provides the total solution, which includes proprietary software; any required hardware; specialised hardware; interfaces to other systems and network cabling.

5.2 All installed components are configured to perform with respective software applications, forming an integral part of the deployed solution. All hardware components are to MoJ and IA approved specification, sourced from MoJ approved suppliers and configured to the IA guidelines as an accreditable solution.

5.3 The maintenance processes is vital to ensure uninterrupted service, optimal system performance and provide the required security features. Unilink can only support and guarantee

the security and performance of components that are sourced, configured, and installed by Unilink.

5.4 Unilink will provide support and maintenance during the Support Agreement term, free of additional charge – as described below and listed in the Hardware Support Table.

5.5 Hardware maintenance does include:

- An unlimited number of support calls during the Contract term
- Replacement and/or repair of a faulty component, supplied by Unilink, is free of charge under warranty, except when fault, or damage is caused by the Buyer's or the Buyer's service users' negligent handling, or deliberate damage by the Buyer or the Buyer's service users;
- On-site repair where possible, or loan replacement if it cannot be repaired onsite;
- Configuration of the components and the system following the repair or replacement;
- Restoration of data, where possible - as part of repair;
- Ensuring that wherever possible equipment is left fully operational following a visit.

5.6 Chargeable Hardware maintenance:

- Supply and installation of consumable items: printer paper rolls, badges, print heads, print and fuser cartridges and UPS batteries;
- Operating Software is not covered and any fixing, visiting or replacements may be chargeable;
- Replacement and/or repair of any components caused by deliberate/accidental damage or negligent handling will be charged;
- Replacement and/or repair of any item beyond the economic life span is chargeable;
- Repair/Support visit following a support call, will be charged if there was no fault found. An authorised site visit request form is required prior to the visit.

6. Typical Hardware Components

➢ Central server is usually the single point of failure for the entire system, housing the database and shared items that the applications, workstations and kiosks connect to. Therefore a 'catastrophic' server failure requires a 6-hours onsite response by an engineer to commence the diagnosis and potential rectification process.

➢ Under IA regulations, servers containing prisoners' and/or staff details and other data on the HDD are not allowed to be removed from Site – for e.g. RTB (return to base) warranty, therefore has to be repaired on-site and in case of HDD replacement the site is responsible to destroy any HDD in accordance with the MoJ security policies & processes.

➢ PCs/Workstations fall under the same restriction as the server. To prevent any potential security issues, repair will be on-site where possible – as above, or the whole PC will be replaced.

➢ UPS – Uninterrupted Power Supply is installed with the server, all PC's and inside Kiosks, it contains a battery to prevent data loss in case of power failure. These are routinely checked during the annual service visit, The batteries inside the UPS are a consumable item and replacement will be charged.

➢ Kiosk devices represent a 'collection' of hardware, i.e. PC, touch screen, fingerprint scanner and printer, housed within a single secure box – therefore an onsite visit by an engineer is sometimes necessary to diagnose and rectify the potential problem.

- ➢ Kiosk touch-screen operation can be affected by dirt/dust and it is the responsibility of the site to perform a regular cleaning regime. Unilink will advise and provide full instructions and training, if required.

Peripheral devices such as fingerprint scanners, printers, cameras etc. will be supported by a 'swap-out' service. A replacement device will be delivered to site to replace the faulty device and it is the site's responsibility to package and send the device or prepare for collection by courier – as advised**.**

7. Annual Audit

7.1 Each site will be audited annually, and the operation of the system checked, confirmed and tested according to Unilink's annual audit procedure at that time.

7.2 The purpose of this visit is to ensure continued healthy system operation. In particular:

- Any discrepancies will be logged;
- System performance will be checked;
- Server and disk performance will be confirmed to be normal;
- Archiving necessary will be carried out in consultation with the Buyer.

7.3 The Account Manager may also visit annually, or on the Buyer's site invitation to:

- Review existing procedures used;
- Review Buyer satisfaction;
- Identify additional training and other requirements.

8. Buyer responsibilities

8.1 The Buyer shall nominate at least one Site Point of Contact (SPOC) for each of its sites to assist with the problem resolution process. The SPOC will have the following responsibilities to assist in rapid fault diagnosis.

8.1.1 for fault rectification, the SPOC must commit to assist with the problem diagnosis to establish the actual cause (network, hardware, software);

8.1.2 in the event of Hardware replacement, the SPOC shall, where requested by Unilink, assist with the siting of the replacement Hardware; and

8.1.3 for Hardware that is returned and swapped out the SPOC will need to package up the relevant Hardware ready for Unilink's courier collection;

8.2 Other responsibilities include:

8.2.1 To clean the equipment in accordance with the operating procedures, particularly kiosk touch-screen, which can be greatly affected by dirt/dust. Unilink will provide cleaning instructions and training, if necessary.

8.2.2. To run and store data backups of the server in accordance with the operating procedures.

8.2.3 To enable access to site for the purposes of maintenance.

8.3 The SPOC shall ensure that the fault diagnosis has been performed according to Unilink's guidance and will authorise the Site Visit Request Form if on-site visit is required. The site visit will be chargeable if no fault was found.

9 Service Desk

9.1 For all software support calls, initial response from a Software Expert will be within 2 hours (1 hour for High severity calls). Support call logging is available 24/7 x 365 days per year.

Technical Support Direct Number: [REDACTED]

9.2 Information Required When Initially Logging a Call.

In order for the Buyer Services to log and allocate all technical support calls efficiently, the following information will be required:

- ✓ The name and telephone number of the person raising the call, or onsite contact if different from the SPOC
- ✓ The software module and functional area if the call is software related.
- ✓ The name, model and serial number of the hardware equipment in question.
- ✓ The location of the hardware with the problem (if applicable).
- ✓ A brief description of the problem along with any associated system error messages.

9.3 A call to the Technical Support number will be answered by the Buyer Service desk. When a call is logged, Unilink will agree a priority with the person logging the call and will provide a call reference number. This number can then be used for both Buyer and Unilink call tracking.

9.4 The Buyer Service desk will log the call, validate the contract information and agree a priority to assign to the call. The Buyer Service desk will then pass this call through to the relevant Software/Technical expert, who will assess current workload provide a response.

9.5 The appropriate expert will then review the call and respond immediately, by telephone, to the problem. The analyst will call upon any resources necessary to resolve the call quickly and efficiently. They may decide that the call needs to be referred to a third party. In this instance, the call will be logged immediately with the third party, who will then contact directly.

Standard Prisons Support and Maintenance

Live Service Support

1. License to use CMS self-service new release at no additional charge during the contracted period.
2. Software patches, new releases and additional modules. New releases are typically published every 3 to 6 months. MOJ will be notified of the content of these releases when the release content has been finalised by Unilink.
3. Unlimited number of calls to the support line, including assistance over the phone
4. Hardware 'swap-out' maintenance of all equipment supplier by Supplier as part of the CMS deployment
5. Annual site visit to check all equipment
6. Additional related service e.g. postcode look up SMS messaging including support and management of the Online Legal Services Visits Booking process and additional web-based services such as links to emails a prisoner, video-visit and payment solutions.
7. User group membership
8. Escrow services to make the software code available in case of disaster recovery or financial distress
9. Support any hardware or software associated with linking to Traka and Gunnebo
10. Second line Support for the Unilink software modules within this Call-Off Contract.

Standard Prisons Hardware Support

For Standard prisons, the Supplier will provide hardware support and maintenance for hardware devices leased by the Standard prisons from the Supplier to the Buyer. These costs will be determined on a case-by-case basis. The overview of maintenance charges and how they are provided is outlined in Schedule 5 below.

Schedule 5: Call-Off Contract charges

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

Self Service Software

For all 27 prisons under this Call-Off Contract, including Digital and Standard Prisons, software is charged at a daily rate based on the total number of beds. The daily rate is [REDACTED], from the go-live date of each prison site.

Hardware Support for Standard Prisons

[REDACTED]

Prices are chargeable on configuration of kiosk/ MoJ signs off acceptance tests.

[REDACTED]

Support charges for these sites are payable monthly, in arrears.

Hardware Support for Digital and In-Cell Technology Prisons

If HMPPS order prisons such that 500 or more additional kiosks are required for installation within one financial year then these kiosks will be supplied at a discount of 20% i.e[REDACTED]per day to reflect the lower manufacturing costs.

Maintenance: In the case of fault, damage or deliberate damage is caused by the Buyer or the Buyer's service users to the Supplier's hardware equipment leased by the Buyer under this Call-Off Contract, the maintenance and repairs costs will be chargeable to the Buyer by the Supplier. This includes replacement and/or repair of one kiosk/ or other equipment per month, resulting from act of vandalism/ malicious by the service users in the prisons in scope of this Call-Off Contract, at the Suppliers expense. Costs for these repairs and maintenance charges are dependent to the scope of damage to the Supplier's hardware, and will include labour and parts charges (all labour charges will align to the Supplier's SFIA Day Rate card as included in Schedule 5 of this Call-Off Contract below.)

There are no additional charges for any faulty hardware equipment that is within warranty. Warranty terms for all hardware equipment can be found in the Hardware Assets table in the Service Level Agreements in Schedule 1.

[REDACTED]

[REDACTED] purchased kiosks directly from Unilink Software Ltd in 2019. The annual charges for hardware support for [REDACTED]

[REDACTED] has pre-paid for three years support fees which apply from go-live of the site. The fees for HMP Bristol do not come within scope of charges under this Call-Off Contract.

SFIA Levels

All the Supplier's team members day rates will align to the Supplier's SFIA Rate Card are outlined below. The rates for each of the Supplier roles are as follows:

1. Supplier technicians who attend prison sites and install Supplier hardware onto the prison walls for use will use a SFIA Level 4 Day Rate.
2. Supplier software engineers who attend prison sites and configure the Supplier software into the Supplier hardware will use a SFIA Level 6 Day Rate.
3. Supplier Developers, to perform any Development work in line with this Call-Off Contract, will use a SFIA Level 6 Day Rate.
4. Supplier project managers will use a SFIA Level 6 Day Rate.
5. The Supplier's Technical Director, in providing services to the Buyer, will use a SFIA Level 7 Day Rate.
6. Any Supplier Training services delivered by the Supplier to the Buyer will be charges at a SFIA Level 6 Day Rate.

All Supplier staff members delivering these services to the Buyer under the terms of this Call-Off Contract will use Capped Time and Materials Charges (Capped T&M charges) as per the SFIA Rate Card for service delivery, throughout this Call-Off Contract and all work packages, and under any extension period to this Call-Off Contract, as per the Supplier's G-Cloud 12 Service Offering 843642414370275. These day rates cannot be amended during this Call-Off Contract unless agreed via a Contract Change Notice (CCN), signed by both Parties in advance of any increase.

[REDACTED]

Standards for Consultancy Day Rate cards

All Supplier staff delivering services to the Buyer in line with services in this Call-Off Contract will follow the Ministry of Justice Travel and Subsistence policy guidance. Information from this guidance shall be provided to the Supplier by the Buyer upon request.

Consultant's Working Day – 7.5 hours exclusive of travel and lunch (our consultants will work a 'professional day' of at least 7.5 hours – hours over 9 hours per day will attract a cost premium of 1.5 times the daily rate as will unsocial hours, Saturdays 1.35 and Sundays 1.5. Partial days will be rounded up to the nearest quarter of a day.

Working Week – Monday to Friday excluding national holidays.

Office Hours - 09:00 – 17:30 Monday to Thursday, 09:00 – 17:00 Friday.

Travel – Travel time is charged at a half-day rate of the relevant Supplier staff members' SFIA Day Rate charges.

Subsistence – Included in day rate for work local to consultant, otherwise charged at [REDACTED]

per day (including hotel, food and telephone costs).

[REDACTED]

Professional Indemnity Insurance – included in day rate

All on-site working must be in a safe environment taking into account the prevalence of Covid-19.

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

Supplier Background IPR – The Supplier's Custodial Management Solution (CMS)

Supplier Project Specific IPR – P-NOMIS API

MOJ Developed Products – Products, documentation and/or software developed by the Buyer that may rely on database structures or data stored in connection with the Supplier Background IPR Software or any New Supplier Products

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 Subject to Clauses 11.9-11.12, the Supplier grants the Buyer a non-exclusive, non-transfer-able, perpetual, irrevocable, royalty-free licence (with the ability to grant sub-licences strictly in connection with the purposes described in Section 11.9(b)) to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities within England and Wales during the Term.

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 where agreed between the Parties and appropriate, 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, without the Buyer's express agreement.

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:

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

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

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

11.9 The Supplier's Background IPR known as the "Custodial Management System " software product, databases and database structures, and related documentation (collectively, the "Supplier Software"), which includes all Background IPR and Project Specific IPR, and all

Services and Deliverables hereunder, consisting of modifications, updates, upgrades, maintenance and support of or to the Supplier Software as previously delivered by the Supplier directly or indirectly to the Buyer or as delivered or permitted under this Agreement (collectively, the "Supplier Software Modifications"), is licensed under the foregoing terms of this Clause 11 with the following modifications set out in this Clause 11.9:

(a) The parties agree that the Supplier Software includes
(i) the product modules previously licensed to the Buyer (which previous licences is fully replaced hereby), including CMS licences at the 27 existing HMPPS prisons listed in this Call-Off Contract.
(ii) all supplier Software Modifications including upgrades thereto.

(b) Without limiting the scope of the license set out in this Clause 11, the Buyer's license includes
(i) the right to properly install, test, trial and conduct acceptance procedures with respect to the Supplier Software,
ii) the right to have an undefined number of concurrent users of the Supplier Software for the management, supervision and administration of adult offenders and any growth in the number of concurrent users thereof and shall also include those youth or young offender facilities currently operated or managed by the Supplier Software,
(iii) the right to conduct such activities that are reasonably required for the Buyer to be able to use the Supplier Software, learn to use it and to maintain and extend the Buyer facilities including training, development and testing activities,
(vi) the right to use the Supplier Software for providing services to or processing data of the Buyer, including providing remote access to the Buyer for purposes permitted hereunder, and performing disaster recovery, disaster testing, back-up and archive as the Buyer deems necessary;

(c) Except as expressly provided in this Agreement, without the prior written consent of the Supplier in its sole discretion, the Buyer may not (and may not permit any person to):
(i) modify, enhance or adapt the Supplier Software or any part of it;
(ii) cause or permit reverse compilation, reverse engineering or reverse assembly of all or any portion of the Supplier Software or any part of it;
(iii) transfer the Supplier Software to any of the three different "Operating Environments" (on-premise for Standard Prisons and Digital Prisons or MoJ Azure Cloud for in-cell technology prisons), being the hardware, operating system software and database software currently (as of the date of this Agreement) used for development and live operation of the Supplier Software (for greater certainty, including the Delivery Platform and the Production System);
(iv) distribute, disclose, market, rent, lease or transfer to any third party any portion of the Supplier Software, or use the Supplier Software in any service bureau arrangement, facility management, or third- party training; or,
(v) transfer, use or sublicense the Supplier Software outside England and Wales;

(d) Notwithstanding Clause 11.3 and Clause 15, and as an express exception thereto;
(i) the Buyer acknowledges and agrees that the source code to the Supplier Software will be considered the Confidential Information of the Supplier, and

the Buyer shall not obtain any rights with respect to the computer code of the Supplier Software and related system documents that are in human-readable form, including all comments and any procedural code such as job control language (the "Source Code") except as provided in this Agreement,

(ii) in particular and notwithstanding the generality of the foregoing, it is expressly acknowledged and agreed that nothing herein shall grant the Buyer any ownership rights in the Supplier Software and the Supplier or its licensors are and shall be the sole owners of the Supplier Software (in both Source Code and executable code form and including Supplier Software Modifications), and the Buyer hereby assigns to the Supplier (including, by this written instrument, as it relates to future-arising works) all right, title and interest (including all Intellectual Property Rights) it may otherwise have but for the provisions of this clause in the Supplier Software, and

(iii) the Buyer shall not, at any time, whether before or after termination of this Agreement contest or aid others in contesting, or doing anything which otherwise impairs the validity of any Intellectual Property Rights, or any right, title or interest of the Supplier in and to the Supplier Software or any portions thereof.

(e) The Buyer's license for the Supplier Software is intended for the sole and exclusive purpose of the administration of criminal offenders which are under the jurisdiction of the Buyer in England and Wales, and it is acknowledged and agreed that, in the event that the statutory responsibility of the Buyer is transferred to another public sector body which will perform its functions, the license shall be deemed to have been transferred to the successor public sector body and, in such event, the Buyer shall give written notice to the Supplier, but no additional charges shall be payable.

11.10 Notwithstanding the foregoing, if a change is requested by the Buyer in accordance with Clause 32, signed by both parties that relates to products, documentation or software not previously offered by the Supplier as part of the Services (the "New Supplier Products"), which will be expressly described in the Contract Change Note (CCN) as "New Supplier Products", the following provisions will apply:

(a) To the extent such CCN relates to any Supplier Software, or Supplier Software Modifications, the foregoing provisions of this Clause 11.1-11.9 shall apply instead of this Clause 11.10 and the Charges shall be as set out in the Order.

(b) Except as set out in Clauses 11.11 and 11.10(a) above, the CCN will expressly state the goals and objectives, scope of work, the parties' roles and responsibilities, and associated costs, and in addition will expressly set out whether any additional Charges relating to the provision of, maintenance of or subscription to the New Supplier Products that apply to the Buyer's use of the New Supplier Products.

(c) Whether or not developed by the Supplier solely, or jointly developed with the Buyer, any New Supplier Products will be owned by the Supplier, and all Intellectual Property Rights therein, in the same manner as it owns the Supplier Software as set out in Clause 11.2 and Clause 11.9, and the Buyer will have the right to use the New Supplier Products as set out in this Clause 11, except as expressly modified by the relevant CCN. Where the Intellectual Property Rights in any New Supplier Products

are the Supplier's Background IPR (other than Supplier Software already licensed under the previous provisions of this Clause 11), then the licence granted by the Supplier to the Buyer shall be agreed by the parties and set out in the CCN.

(d) As an express exception to Clause 11.3 and Clause 15, notwithstanding any joint efforts in developing the New Supplier Products, the Buyer acknowledges and agrees that the Source Code to the New Supplier Products will be considered the Confidential Information of the Supplier and the Buyer will not disclose any New Supplier Product Source Code except as expressly agreed by the Supplier in writing (in its sole discretion), subject always to Clause 10.1 and the relevant provisions of the Framework Agreement.

(e) Without prejudice to clause 11.2, except as it relates to any Buyer Confidential Information and/or data and material provided by the Buyer that may be used in connection with the development of the New Supplier Products (which will be deemed licensed to Supplier in a manner consistent with, and subject to the limitations of, Clause 11.11(d)(ii) below), the Buyer hereby assigns (including, by this written instrument, as it relates to future-arising works) all right, title and interest (including all Intellectual Property Rights), in and to the New Supplier Products to Supplier, and hereby waives all moral rights therein and thereto.

11.11 Notwithstanding the foregoing, if the Supplier and the Buyer enter into a Contract Change Notice (CCN) signed by both Parties in accordance with Clause 32 of this Call-Off Contract, that relates to products, documentation or software that may rely on database structures or data stored in connection with the Supplier Software or any New Supplier Products (the "MOJ-Developed Products"), which will be expressly described in the CCN as "MoJ-Developed Products", the following provisions will apply.

(a) To the extent such CCN relates to any Supplier Software Modifications, or modifications to New Supplier Products the foregoing provisions of this Clause 11 shall apply instead of this Clause 11.11.

(b) Except as set out in (a) above, the CCN will expressly state the goals and objectives, scope of work, the parties' roles and responsibilities, but the Buyer will be responsible for the costs associated with the development, testing and use of MOJ-Developed Products except as otherwise agreed in the CCN.

(c) The Buyer acknowledges and agrees that

(i) the Buyer will have primary responsibility for managing any project to develop or deploy MOJ-Developed Products;

(ii) the Buyer will not be permitted to alter any database or database structure in belonging to the Supplier as part of the Supplier Software or New Supplier Products (the "Underlying Databases");

(iii) the Supplier recommends use of Supplier application programming interfaces in accordance with the Supplier's documentation provided as part of the existing Services for all access to its Underlying Databases; and,

(iv) if any maintenance or support is needed to the Supplier Software or New Supplier Products as a direct result of the Buyer failing to follow any

reasonable requirements of the Supplier with regards the interface between the MOJ-Developed Products and the Supplier Software, New Supplier Products, or Underlying Databases, the Supplier shall not be responsible for such maintenance or support as part of its provision of the Services. Any requirement on the Supplier to provide such maintenance and support shall be commissioned through a new CCN.

(d) The Variation/ CCN will expressly set out the ownership of the Intellectual Property Rights of the MOJ-Developed Products, but in the absence of that:

(i) with or without the assistance of the Supplier, the Buyer will own the MOJ-Developed Products and all Intellectual Property Rights therein;

(ii) to the extent not consisting of Confidential Information of the Supplier, the Supplier hereby assigns (including, by this written instrument, as it relates to future-arising works) all right, title and interest (including all Intellectual Property Rights and the ability to publish any source code), in and to the MOJ-Developed Products to the Buyer, and hereby waives all moral rights therein and thereto; and,

(iii) the Buyer will grant to Supplier a non-exclusive, worldwide, royalty-free right and license to use, load, execute, store, transmit, display, modify, adapt, translate or otherwise utilize and exploit the MOJ-Developed Products (in executable and Source Code form) in connection with the Supplier's provision of the Services (including the provision of any New Supplier Products, Supplier Software Modifications, and assistance with the MOJ-Developed Products). This licence shall also permit the Supplier to use the MOJ-Developed Product in developing other products, services or offerings to other customers provided that any Buyer Confidential Information shall not be used by the Supplier in developing such products, services or offerings to other customers and the Supplier shall indemnify the Buyer from and against all Losses arising from any breach of this obligation;

(iv) where the Buyer waives their rights to the IPR of such products, the Supplier will incorporate such new developments into the CMS package of products and supply them, including support, at no additional charge. Where the Buyer retains the IPR of new products if the Supplier is required to support them this will be offered at additional charge by the Supplier to the Buyer.

(e) The Supplier will promptly respond to all reasonable requests relating to the entry of a CCN for an MoJ-Developed Product as contemplated by this Clause 11.11, but if the Supplier is unable or unwilling to do so on terms reasonably acceptable to both Parties, the Supplier acknowledges and agrees that the Buyer shall have the right (without assistance of the Supplier, and without liability to the Supplier) to develop MoJ-Developed Products strictly in accordance with subsections (c) through (e) above, but will notify the Supplier thereof in writing and provide such reasonable information regarding the MoJ-Developed Products so as to permit the Supplier to exercise its rights under this Agreement. Nothing in this clause 11.11(e) prevents the Buyer developing products unrelated to the Supplier's software with third parties without reference to the Supplier.

(f) Nothing in this Section 11.11 affects Supplier's rights, titles or interests in or to any Supplier Software or New Supplier Products.

11.12 In addition to Clause 11.7, Clause 11.5 will not apply if the IPR Claim is from:

(a) the Supplier's compliance with specifications or express requirements provided by the Buyer, where the Supplier has provided written notice to the Buyer, that the Buyer's proposed specifications or express requirements might lead to an IPR Claim and the Buyer has ignored this notice;

(b) additions to or modifications of any Deliverable or Service, or any Background IPR or Project Specific IPR, by the Buyer or any third party not authorized by the Supplier;
(c) use of any Deliverable or Service, or any Background IPR or Project Specific IPR, in combination with any other products, equipment, devices, software, systems or data not supplied or authorized in writing (including in any documentation) by the Supplier; or

(d) the use of any Deliverable or Service, or any Background IPR or Project Specific IPR, that is not permitted by this Agreement.

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 committed, 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 use of HMPPS's data by the Buyer (the Authority) will be used as required by HMPPS throughout this Call-Off Contract. This will start from the Call-Off Contract Start Date to the Call-Off Contract End Date. If this Call-Off Contract is terminated before the Call-Off Contract End Date, the final date of the processing of HMPPS's Data will cease on the amended Call-Off Contract End Date. If there is no extension to this Call-Off Contract, the final date for processing HMPPS's data will be the Contract Exit date, 15th April 2022. 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	The data to be processed includes biometric data to help identify prisoners and provide access control to kiosks.
Type of Personal Data	The Type of Personal Data under this Call-Off Contract will be: • The Custodial sentence terms, including the crime committed, 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	This Data relates to: • 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 plan for the return and destruction of data will be included as part of the Supplier's Exit Plan from this Call-Off Contract, as outlined above in this Order Form. The Buyer's Exit Manager will lead this management on behalf of the Buyer. The Buyer's Data shall be retained by the Supplier during third line support investigations then destroyed by the Supplier on behalf of the Buyer. The Buyer will provide the Supplier instructions the plan for the return and destruction of Buyer

	personal data and the responsibilities of both Parties within 90 days of the Call-Off Contract Start Date. This will include confirmation of the date of the Supplier's destruction of the Buyer's data. The Supplier will provide the Buyer with a data destruction certificate relating to personal data destroyed by the Supplier within the time period agreed.

Schedule 8 – Work Packages

Date of Work Package:	
Work Package Reference:	**Con_XXXXX Work Package_XX**
Services this Work Package is delivering	
Buyer:	*The Secretary of State for Justice on behalf of Her Majesty's Prisons and Probation Services*
Supplier:	Unilink Software Limited
Release Type(s):	
Development Requirement:	
Start Date of Work Package:	
End Date of Work Package:	
Charging Method(s) for this Release:	Payment method will be Time and materials (T&M), based on completion of individual Work Package, in line with Schedule 5 of this Call-Off Contract.
PO Number to be Used	

The Parties will execute a Work Package (WP) as required for development work. All development work and ad-hoc Service requirements are to be agreed between both Parties in advance of any services being delivered. The Parties may agree these services via email confirmation, and then the Parties shall amend and update the current Work Package in respect of these services.

The rights, obligations and details agreed by the Parties and set out in this Work Package apply only in relation to the Services that are to be delivered under this Work Package and will not apply to any other Work Packages executed or to be executed under this Call-Off Contract unless otherwise agreed by the Parties.

Deliverables

The Parties agree that the Deliverables provided by the Supplier in respect of this/ these Project(s) are detailed in the table below:

Services Requested	Deliverables	Acceptance Criteria

More detailed plans and outcomes will be defined with the programme on a monthly basis, being guided by the Work Packages. Any changes to the services delivered under this Work Package will be reflected as an amendment to the Work Package.

Any work for which a proportion fails to meet the Acceptance Criteria in a specified period will not be accepted by the Buyer and will be completed at the Supplier's expense. The Charges applied to that proportion of work will be excluded from the total Charges due for that period. Those Charges so excluded may only be charged once the quality and standard of the work for that period has been accepted by the Buyer.

Key Specialist Roles:

The table below reflects the specialist roles and teams who will be working on to support the delivery of the above services for the next 3 months:

Specialist Role	Team	Services to be Delivered by Specialist

Additional Service Level Agreements under this Work Package 00X

Specific service level agreements for this Work Package are agreed by the Supplier with the Buyer. This includes specific service level agreements for roles to be provided within this Work Package. Additional Service Level Agreements for this Work Package are listed below:

Role	Service Level Agreement	Target Resolution

The additional service level agreements may not be applicable to all Work Packages and may apply to this Work Package only.

Risks

Risk	Mitigating action

Call-Off Contract Charges

For each individual Work Package (WP), the applicable Call-Off Contract Charges (in accordance with the charging method in the Order Form) will be calculated using all of the following:

- the agreed relevant rates for Supplier staff or facilities, which are Exclusive of any applicable expenses and exclusive of VAT and which were submitted to the Buyer during the Further Competition that resulted in the award of this Call-Off Contract.
- The number of days, or pro rata for every part of a day, that Supplier staff or facilities will be actively providing the Services during the term of the Work Package

The detailed breakdown for the provision of Services during the term of the Work Package will include (but will not be limited to):

Supplier Specialist Role	Role Description	Rate	Start Date	End Date	Total Costs
Total Cost of Work Package					

Note: The Start Date and the End Date, and work effort (number of days) of each Specialist role are a best estimate of service delivery days, and therefore a best estimate of costs for the delivery of these services per Specialist role. It is the responsibility of the Supplier to advise to the Buyer when the Buyer is within 25% of the capped spend for this Work Package.

Any work for which a proportion fails to meet the Acceptance Criteria in a specified period will not be accepted by the Buyer and will be completed at the Supplier's expense. The Charges applied to that proportion of work will be excluded from the total Charges due for that period. Those Charges so excluded may only be charged once the quality and standard of the work for that period has been accepted by the Buyer.

Service Lead Approval will be received from the designated Service Lead on behalf of HMPPS Digital.

For confirming these services have been delivered and may be paid via invoice, approval will be received from the designated Service Lead on behalf of HMPPS Digital.

The Parties may agree ad hoc services via email confirmation, and then the Parties shall amend and update the current Work Package in respect of these ad hoc services. This will not require a Contract Change Notice to be put into place.

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

For and on behalf of Unilink Software Ltd:

Name and title .....

Signature and date .....

For and on behalf of HMPPS Digital:

Name and title .....

Signature and date .....

For and on behalf of the Ministry of Justice Commercial and Contract Management Directorate (CCMD):

Name and title .....

Signature and date .....

If you exceed the overall Call-Off Contract value and Supplier Staff are still required to deliver the services, then a contract change note (CCN) must be raised, explaining the reason(s) for the extension.