

# G-Cloud 11 Call-Off Contract (version 4)

**Contents**

[G-Cloud 11 Call-Off Contract (version 4) 1](#_Toc18482982)

[**Part A - Order Form** 3](#_Toc18482983)

[**Schedule 1 – Services** 10](#_Toc18482984)

[**Schedule 2 - Call-Off Contract charges** 11](#_Toc18482985)

[**Part B - Terms and conditions** 12](#_Toc18482986)

[**Schedule 3 - Collaboration agreement** 33](#_Toc18482987)

[**1. Definitions and interpretation** 34](#_Toc18482988)

[**2. Term of the agreement** 35](#_Toc18482989)

[**3. Provision of the collaboration plan** 35](#_Toc18482990)

[**4. Collaboration activities** 36](#_Toc18482991)

[**5. Invoicing** 36](#_Toc18482992)

[**6. Confidentiality** 36](#_Toc18482993)

[**7. Warranties** 37](#_Toc18482994)

[**8. Limitation of liability** 37](#_Toc18482995)

[**9. Dispute resolution process** 38](#_Toc18482996)

[**10. Termination and consequences of termination** 39](#_Toc18482997)

[**11. General provisions** 39](#_Toc18482998)

[**Schedule 4 - Alternative clauses** 43](#_Toc18482999)

[**1. Introduction** 43](#_Toc18483000)

[**2. Clauses selected** 44](#_Toc18483001)

[**Schedule 5 - Guarantee** 44](#_Toc18483002)

[**Schedule 6 - Glossary and interpretations** 45](#_Toc18483003)

[**Schedule 7 - GDPR Information** 53](#_Toc18483004)

[**Schedule 8 – Software** 77](#_Toc18483005)

## **Part A - Order Form**

|  |  |
| --- | --- |
| **Digital Marketplace service ID number:** | 375923700153280 |
| **Call-Off Contract reference:** | TIS0323 |
| **Call-Off Contract title:** | Business World Licencing and Support |
| **Call-Off Contract description:** | Provision of SaaS Licencing and Support for Business World. |
| **Start date:** | 28th July 2019 |
| **Expiry date:** | 27th July 2021 (with two allowed 12 month extensions to 27th July 2023) |
| **Call-Off Contract value:** | £2,500,000 (including all extension options) |
| **Charging method:** | BACS |
| **Purchase order number:** |  |

This Order Form is issued under the G-Cloud 11 Framework Agreement (RM1557.11).

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** | Insolvency Service  Buyer’s main address:  Canon House  Birmingham  B4 6FD |
| **To: the Supplier** | Agilisys Limited  Telephone: REDACTED  Supplier’s address:  REDACTED  Company number:  04327369 |
| **Together: the ‘Parties’** | |

### Principle contact details

|  |  |
| --- | --- |
| **For the Buyer:** | Title: Financial and Commercial Director  Name: REDACTED  Email: REDACTED  Phone: REDACTED |
| **For the Supplier:** | Title: Partner  Name: REDACTED  Email: REDACTED  Phone: REDACTED |

### Call-Off Contract term

|  |  |
| --- | --- |
| **Start date:** | This Call-Off Contract is deemed to have commenced on 28 July 2019 and is valid for 24 months |
| **Ending (termination):** | The notice period needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums or at least 365 days from the date of written notice for Ending without cause. .  For the avoidance of doubt these notice provision do not apply to the Extension Period. |
| **Extension period:** | This Call-Off Contract can be extended by the Buyer for 2 period(s) of 12 months each, by giving the Supplier 3 months written notice before its expiry.  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 and Supplier to confirm provisions on exit on Supplier sufficient to satisfy any additional exit plan arrangements |

### Buyer contractual details

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

|  |  |
| --- | --- |
| **G-Cloud lot:** | This Call-Off Contract is for the provision of Services under  Lot 2 - Cloud software  Lot 3 - Cloud support |
| **G-Cloud services required:** | The Services to be provided by the Supplier under Service ID 375923700153280 and outlined below:  Access to the Unit4 Software as a Service subject to the terms included on the Unit4 Portal. The specific SaaS modules being detailed within Schedule 8;  Additional licences by both module and user type may be procured by agreement to meet future demand from the Buyer. Cloud Hosting of Software See Appendix E and Appendix F of Unit4 terms.Software Support Services - Premium Support; See Appendix C of Unit4 terms. The Supplier shall provide: Telephone based help and advice in the use of the Software;Standard software fault reporting and fixing service; Enhancement request service; |
| **Additional Services:** | Call-off support services to the Buyer on request via change control. This shall include the provision of highly skilled staff to provide Unit4 Business World development, integrations, change management.  The following Additional services shall be subject to additional costs which are not covered under the Agreement and shall be quoted to the Buyer: Additional consultancy support from the Supplier will be offered on a call-off basis as part of this contract to support the discovery, design and delivery of Unit 4 Business World projects.   This will include known planned projects as set out below:   * Breathing Space/SDRP * SIAM   This may also include future projects relating to Unit 4 Business World configuration, integration and upgrades.  The Supplier will work collaboratively with the Buyer to agree a scope of works for the discovery phases on a time and materials basis. Following the Discovery Phase, the Buyer will make a Go/No-Go decision relating to the Supplier delivering this integration, with milestones and deliverables to be agreed as a Fixed Price activity during Live delivery of the Services.  Licence Offer:  Licence offer for additional 40 professional users which will also upgrade all existing self-service users to professional users will be held until 1st December 2019 at the price of REDACTED per annum (subject to indexation thereafter). |
| **Location:** | The Services will be delivered to Cannon House, Birmingham, B4 6FD.  Software Services will be delivered using:  Subcontractor Unit4 support service centres, which are based in Poland and Bristol.  Subcontractor Unit4 Cloud Services - delivered by Unit4 utilizing Microsoft Azure data centres within Europe. |
| **Quality standards:** | The quality standards required for this Call-Off Contract as described in the service description documentation Appendix E and F which can be found on the Supplier G-Cloud Portal |
| **Technical standards:** | The technical standards required for this Call-Off Contract as  described in the service description documentation Appendix E and F which can be found on the Supplier G-Cloud Portal |
| **Service level agreement:** | The service level and availability criteria required for this Call-Off Contract are As described in the service description documentation Appendix E and F which can be found on the Supplier G-Cloud Portal Appendix D describes the SLA’s that will apply. |
| **Onboarding:** | N/A as an extension to a current SaaS |
| **Offboarding:** | Upon final exit the Supplier will export the final copy of the Production Database to a controlled Azure storage location provided that a request has been received 7 business days prior to the date the export copy is required. The export will be in the native database format which should be a format usable with the latest version of Microsoft SQL Server. Customers can manually download this export from this location. Customer responsibilities for this additional service offering include: • Customer access responsibility – control who has permission to download the export • Ensuring data privacy during and after download • Establishing, monitoring and managing the download process • Restoring or importing the export once downloaded • Licensing, operating and installing in the customer’s IT infrastructure any applications that will be used in the retrieval process and subsequent use of the export |
| **Collaboration agreement:** | N/A |
| **Limit on Parties’ liability:** | The annual total liability of either Party for all Property defaults will not exceed 100% of the value of the contract annual charges.  The annual total liability for Buyer Data defaults will not exceed 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term .  The annual total liability for all other defaults will not exceed 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term |
| **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 £2,000,000 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 30 consecutive days. |
| **Audit:** | N/A |
| **Buyer’s responsibilities:** | The Buyer is responsible for complying with all Buyers Responsibilities set out in the Unit4 Terms and Conditions including, without limitation, clause 5.4 of Appendix A, Clause 6 of Appendix A and Unit4’s Acceptable Use Policy on www.unit4.com/terms |
| **Buyer’s equipment:** | Not Applicable |

### Supplier’s information

|  |  |
| --- | --- |
| **Subcontractors or partners:** | The following is a list of the Supplier’s Subcontractors or Partners   * Unit 4 (for Software Services). |

### 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   | **Milestone** | **Date** | **Value** | | --- | --- | --- | | Annual SaaS | 28th July 2019 | REDACTED | | Annual SaaS | 28th July 2020 | REDACTED | | Annual SaaS | 28th July 2021 | REDACTED | | Annual SaaS | 28th July 2022 | REDACTED |   ¹All charges are exclusive of VAT  ² Subject to annual indexation |
| **Invoice details:** | The Supplier will issue electronic invoices annually in advance. 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 |
| **Invoice information required** – for example purchase order, project reference: | All invoices must include a copy of approved timesheets and Certificates of Acceptance for deliverables/milestones if applicable. Payment of SaaS shall not be conditional on any form of Certificate Acceptance The Purchase Order Number shall be quoted on all invoices to be valid. |
| **Invoice frequency:** | Invoice will be sent to the Buyer annually for SaaS and monthly for any other Services. |
| **Call-Off Contract value:** | £2,500,000 |
| **Call-Off Contract charges:** | The breakdown of the Charges is set out below:   | **Milestone** | **Date** | **Value** | | --- | --- | --- | | Annual SaaS (including Premium Support) | 28th July 2019 | REDACTED | | Annual SaaS (including Premium Support) | 28th July 2020 | REDACTED | | Annual SaaS (including Premium Support) | 28th July 2021 | REDACTED | | Annual SaaS (including Premium Support) | 28th July 2022 | REDACTED |   ¹All charges are exclusive of VAT  ² Subject to annual indexation  SFIA Day Rates are outlined in Schedule 2. |

### Additional Buyer terms

|  |  |
| --- | --- |
| Performance of the service and deliverables: | The SaaS Service is provided in accordance with Unit4 Service Descriptions Appendix E and F and the Service Level Agreement Appendix D. Support in all cases is based on Appendix C – Unit4’s Tiered Support Terms |
| Guarantee: | Not used. |
| Warranties, representations: | N/A |
| Supplemental requirements in addition to the Call-Off terms: | N/A |
| Alternative clauses: | Please see Schedule 4 |
| Buyer specific amendments to/refinements of the Call-Off Contract terms: | N/A |
| Public Services Network (PSN): | N/A |
| Personal Data and Data Subjects: | The Supplier is the Processor of data for the Buyer with Unit4 a sub-processor of the Buyer who will process data in respect of **only** the services provided by the sub-processor in accordance with the terms of this Agreement and the data processing information in Schedule 7. |

**1. Formation of contract**

1. By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.
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.
3. This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
4. In cases of any ambiguity or conflict the terms and conditions of the Call-Off Contract and Order Form will supersede those of the Supplier Terms and Conditions.

**2. Background to the agreement**

1. The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.11.
2. The Buyer provided an Order Form for Services to the Supplier.

|  |  |  |
| --- | --- | --- |
| **Signed:** | Supplier | Buyer |
| **Name:** | REDACTED | REDACTED |
| **Title:** | Managing Director | Finance and Commercial Director |
| **Signature:** |  |  |
| **Date:** |  |  |

## **Schedule 1 – Services**

1. The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:

### Access to the Unit4 Software as a Service is provided subject to the Unit4 terms included on the Unit4 Portal. The specific Software modules being purchased are detailed within Schedule 8;

* 1. Additional licences by both module and user type may be procured by agreement to meet future demand from the Buyer.

### Cloud Hosting of Software;

### Software Support Services - Premium Support;

1. The Supplier shall provide:

#### Telephone based help and advice in the use of the Software;

#### Software fault reporting and fixing service;

#### Enhancement request service;

#### Support Services.

### The Supplier shall be able to provide Call-Off Support Services to deliver a range of activities including Development of Software for the Buyer, Configuration activities, Integration with other systems, ad hoc support for small projects or BAU activities etc. These services to be agreed via Change Control.

### The Supplier shall continue the delivery of the Breathing Space/SDRP Discovery phase and if instructed and accepted under change control shall price and deliver the full implementation of Breathing Space/SDRP project as required. Costs for this shall be agreed between the Parties.

### The Supplier shall provide an Account Manager who shall be responsible for managing all performance related activities and act as the initial escalation point for the Buyer.

### The account manager shall attend monthly performance meetings with the Buyer and the SIAM supplier. These meetings shall take place at the Cannon House, Birmingham, B4 6FD, attendance may be virtual or in person.

## **Schedule 2 - Call-Off Contract charges**

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

REDACTED

These prices are exclusive of VAT. Travel and subsistence are included in these day rates for travel within M25. Travel and subsistence will be payable at our standard rates outside of the M25.

This does not apply to travel and subsistence for our 3rd party suppliers, which will be treated as exclusive of their rates.

## **Part B - Terms and conditions**

### 1. Call-Off Contract start date and length

1. The Supplier must start providing the Services on the date specified in the Order Form.
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.
3. The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.
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

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)
   * 8.4 (Relationship)
   * 8.7 to 8.9 (Entire agreement)
   * 8.10 (Law and jurisdiction)
   * 8.11 to 8.12 (Legislative change)
   * 8.13 to 8.17 (Bribery and corruption)
   * 8.18 to 8.27 (Freedom of Information Act)
   * 8.28 to 8.29 (Promoting tax compliance)
   * 8.30 to 8.31 (Official Secrets Act)
   * 8.32 to 8.35 (Transfer and subcontracting)
   * 8.38 to 8.41 (Complaints handling and resolution)
   * 8.42 to 8.48 (Conflicts of interest and ethical walls)
   * 8.49 to 8.51 (Publicity and branding)
   * 8.52 to 8.54 (Equality and diversity)
   * 8.57 to 8.58 (data protection)
   * 8.62 to 8.63 (Severability)
   * 8.64 to 8.77 (Managing disputes and Mediation)
   * 8.78 to 8.86 (Confidentiality)
   * 8.87 to 8.88 (Waiver and cumulative remedies)
   * 8.89 to 8.99 (Corporate Social Responsibility)
   * paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
   * any audit provisions from the Framework Agreement set out by the Buyer in the Order Form
2. The Framework Agreement provisions in clause 2.1 will be modified as follows:
   * a reference to the ‘Framework Agreement’ will be a reference to the ‘Call-Off Contract’
   * a reference to ‘CCS’ will be a reference to ‘the Buyer’
   * a reference to the ‘Parties’ and a ‘Party’ will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract
3. The Parties acknowledge that they are required to complete the applicable Annexes contained in schedule 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.
4. The Framework Agreement incorporated clauses will be referred to as ‘incorporated Framework clause XX’, where ‘XX’ is the Framework Agreement clause number.
5. When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

### 3. Supply of services

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.
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

1. The Supplier Staff must:
   * be appropriately experienced, qualified and trained to supply the Services
   * apply all due skill, care and diligence in faithfully performing those duties
   * obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
   * respond to any enquiries about the Services as soon as reasonably possible
   * complete any necessary Supplier Staff vetting as specified by the Buyer
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.
3. The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
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.
5. The Buyer may End this Call-Off Contract for Material Breach if the Supplier is delivering the Services Inside IR35.
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.
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.
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

1. Both Parties agree that when entering into a Call-Off Contract they:
   * have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
   * are confident that they can fulfil their obligations according to the Call-Off Contract terms
   * have raised all due diligence questions before signing the Call-Off Contract
   * have entered into the Call-Off Contract relying on its own due diligence

### 6. Business continuity and disaster recovery

1. The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.
2. The Supplier’s business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
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

1. The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier’s delivery of the Services.
2. The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
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.
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.
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.
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. All Charges payable by the Buyer to the Supplier will include VAT at the appropriate rate.
8. The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
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.
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.
11. If there’s an invoice dispute, the Buyer must pay the undisputed 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.
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

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

### 9. Insurance

1. The Supplier will maintain the insurances required by the Buyer including those in this clause.
2. The Supplier will ensure that:
   * during this Call-Off Contract, Subcontractors hold third­party 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
   * the third-party public and products liability insurance contains an ‘indemnity to principals’ clause for the Buyer’s benefit
   * 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
   * 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
3. If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
4. If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
   * a broker's verification of insurance
   * receipts for the insurance premium
   * evidence of payment of the latest premiums due
5. Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
   * + take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
     + promptly notify the insurers in writing of any relevant material fact under any insurances
     + hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance
6. The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
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.
8. The Supplier will be liable for the payment of any:
   * premiums, which it will pay promptly
   * excess or deductibles and will not be entitled to recover this from the Buyer

### 10. Confidentiality

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 8.78 to 8.86. The indemnity doesn’t apply to the extent that the Supplier breach is due to a Buyer’s instruction.

### 11. Intellectual Property Rights

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.
2. The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer’s ordinary business activities.
3. The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer’s right to publish the IPR as open source.
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.
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
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
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
8. If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

### 12. Protection of information

1. The Supplier must:
   * comply with the Buyer’s written instructions and this Call-Off Contract when Processing Buyer Personal Data
   * 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
   * take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes
2. The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:
   * providing the Buyer with full details of the complaint or request
   * complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer’s instructions
   * providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
   * providing the Buyer with any information requested by the Data Subject
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

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

1. The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.
2. If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.
3. 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 policy and all Buyer requirements in the Order Form.
4. The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
5. The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:
   * the principles in the Security Policy Framework at <https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy at <https://www.gov.uk/government/publications/government-security-classifications>
   * guidance issued by the Centre for Protection of National Infrastructure on Risk Management at <https://www.cpni.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets at <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
   * the National Cyber Security Centre’s (NCSC) information risk management guidance, available at <https://www.ncsc.gov.uk/collection/risk-management-collection>
   * government best practicei[n](https://www.cesg.gov.uk/risk-management-collection) [t](https://www.cesg.gov.uk/risk-management-collection)he design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
   * the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>
6. The Buyer will specify any security requirements for this project in the Order Form.
7. 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.
8. 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.
9. 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

1. The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.
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 available at](https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary) <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
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.
4. If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
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[.](https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary)

### 15. Open source

1. All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.
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

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.
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.
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.
4. Responsibility for costs will be at the:
   * 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
   * 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
5. The Supplier will immediately notify CCS of any breach of security of CCS’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 CCS and Buyer Confidential Information however it may be recorded.
6. Any system development by the Supplier should also comply with the government’s ‘10 Steps to Cyber Security’ guidance, available at <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
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

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:
   * an executed Guarantee in the form at Schedule 5
   * 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

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.
2. The Parties agree that the:
   * Buyer’s right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
   * If the Buyer Ends this Call-Off Contract under clause 18.1, the Buyer shall remain liable to pay the Charges in full for the remainder of the then current contracted Term.
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.
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:
   * a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
   * any fraud
5. A Party can End this Call-Off Contract at any time with immediate effect by written notice if:
   * 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
   * an Insolvency Event of the other Party happens
   * the other Party ceases or threatens to cease to carry on the whole or any material part of its business
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.
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

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.
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.
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.
4. Ending or expiry of this Call-Off Contract will not affect:
   * any rights, remedies or obligations accrued before its Ending or expiration
   * the right of either Party to recover any amount outstanding at the time of Ending or expiry
   * 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); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.87 to 8.88 (Waiver and cumulative remedies)
     + 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
5. At the end of the Call-Off Contract Term, the Supplier must promptly:
   * return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
   * return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
   * 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
   * 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
   * work with the Buyer on any ongoing work
   * return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date
6. Each Party will return all of the other Party’s Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.
7. All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

### 20. Notices

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** | **Deemed time of delivery** | **Proof of service** |
| Email | 9am on the first Working Day after sending | Sent by pdf to the correct email address without getting an error message |

1. 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

1. The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
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.
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.
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.
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.
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:
   * 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
   * there will be no adverse impact on service continuity
   * there is no vendor lock-in to the Supplier’s Service at exit
   * it enables the Buyer to meet its obligations under the Technology Code Of Practice
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.
8. The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
   * 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
   * 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
   * the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
   * the testing and assurance strategy for exported Buyer Data
   * if relevant, TUPE-related activity to comply with the TUPE regulations
   * 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

1. At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:
   * data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier’s possession, power or control
   * other information reasonably requested by the Buyer
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.
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

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

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:
   * Property: for all defaults 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
   * Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
   * Other defaults: for all other defaults, 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

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.
2. The Supplier will use the Buyer’s premises solely for the performance of its obligations under this Call-Off Contract.
3. The Supplier will vacate the Buyer’s premises when the Call-Off Contract Ends or expires.
4. This clause does not create a tenancy or exclusive right of occupation.
5. While on the Buyer’s premises, the Supplier will:
   * comply with any security requirements at the premises and not do anything to weaken the security of the premises
   * comply with Buyer requirements for the conduct of personnel
   * comply with any health and safety measures implemented by the Buyer
   * immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury
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

1. The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.
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.
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

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

1. The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.
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)

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.
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:
   * the activities they perform
   * age
   * start date
   * place of work
   * notice period
   * redundancy payment entitlement
   * salary, benefits and pension entitlements
   * employment status
   * identity of employer
   * working arrangements
   * outstanding liabilities
   * sickness absence
   * copies of all relevant employment contracts and related documents
   * all information required under regulation 11 of TUPE or as reasonably requested by the Buyer
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.
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.
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.
6. The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
   * its failure to comply with the provisions of this clause
   * 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
7. The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
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

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.
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

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.
2. In addition to any obligations under the Collaboration Agreement, the Supplier must:
   * work proactively and in good faith with each of the Buyer’s contractors
   * 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

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.
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.
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 8.57 and 8.58 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 8.57 and 8.58 are reproduced in this Call-Off Contract document at schedule 7

## **Schedule 3 - Collaboration agreement**

This agreement is made on [enter date]

between:

1. [Buyer name] of [Buyer address] (the Buyer)
2. [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]
3. [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]
4. [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]
5. [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]
6. [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

together (the Collaboration Suppliers and each of them a Collaboration Supplier).

Whereas the:

* Buyer and the Collaboration Suppliers have entered into the Call-Off Contracts (defined below) for the provision of various IT and telecommunications (ICT) services
* Collaboration Suppliers now wish to provide for the ongoing cooperation of the Collaboration Suppliers in the provision of services under their respective Call-Off Contract to the Buyer

In consideration of the mutual covenants contained in the Call-Off Contracts and this Agreement and intending to be legally bound, the parties agree as follows:

## **1. Definitions and interpretation**

1. As used in this Agreement, the capitalised expressions will have the following meanings unless the context requires otherwise:
   * “Agreement” means this collaboration agreement, containing the Clauses and Schedules
   * “Call-Off Contract” means each contract that is let by the Buyer to one of the Collaboration Suppliers
   * “Contractor’s Confidential Information” has the meaning set out in the Call-Off Contracts
   * “Confidential Information” means the Buyer Confidential Information or any Collaboration Supplier's Confidential Information
   * “Collaboration Activities” means the activities set out in this Agreement
   * “Buyer Confidential Information” has the meaning set out in the Call-Off Contract
   * “Default” means any breach of the obligations of any Collaboration Supplier or any default, act, omission, negligence or statement of any Collaboration Supplier, its employees, servants, agents or subcontractors in connection with or in relation to the subject matter of this Agreement and in respect of which such Collaboration Supplier is liable (by way of indemnity or otherwise) to the other parties
   * “Detailed Collaboration Plan” has the meaning given in clause 3.2
   * “Dispute Resolution Process” means the process described in clause 9
   * “Effective Date” means deemed as of 28July 2019
   * “Force Majeure Event” has the meaning given in clause 11.1.1
   * “Mediator” has the meaning given to it in clause 9.3.1
   * “Outline Collaboration Plan” has the meaning given to it in clause 3.1
   * “Term” has the meaning given to it in clause 2.1
   * "Working Day" means any day other than a Saturday, Sunday or public holiday in England and Wales
2. General
   1. As used in this Agreement the:
      1. masculine includes the feminine and the neuter
      2. singular includes the plural and the other way round
      3. A reference to any statute, enactment, order, regulation or other similar instrument will be viewed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent re-enactment.
   2. Headings are included in this Agreement for ease of reference only and will not affect the interpretation or construction of this Agreement.
   3. References to Clauses and Schedules are, unless otherwise provided, references to clauses of and schedules to this Agreement.
   4. Except as otherwise expressly provided in this Agreement, all remedies available to any party under this Agreement are cumulative and may be exercised concurrently or separately and the exercise of any one remedy will not exclude the exercise of any other remedy.
   5. The party receiving the benefit of an indemnity under this Agreement will use its reasonable endeavours to mitigate its loss covered by the indemnity.

## **2. Term of the agreement**

* 1. This Agreement will come into force on the Effective Date and, unless earlier terminated in accordance with clause 10, will expire 6 months after the expiry or termination (however arising) of the exit period of the last Call-Off Contract (the “Term”).
  2. A Collaboration Supplier’s duty to perform the Collaboration Activities will continue until the end of the exit period of its last relevant Call-Off Contract.

## **3. Provision of the collaboration plan**

* 1. The Collaboration Suppliers will, within 2 weeks (or any longer period as notified by the Buyer in writing) of the Effective Date, provide to the Buyer detailed proposals for the Collaboration Activities they require from each other (the “Outline Collaboration Plan”).
  2. Within 10 Working Days (or any other period as agreed in writing by the Buyer and the Collaboration Suppliers) of [receipt of the proposals] or [the Effective Date], the Buyer will prepare a plan for the Collaboration Activities (the “Detailed Collaboration Plan”). The Detailed Collaboration Plan will include full details of the activities and interfaces that involve all of the Collaboration Suppliers to ensure the receipt of the services under each Collaboration Supplier’s respective [contract] [Call-Off Contract], by the Buyer. The Detailed Collaboration Plan will be based on the Outline Collaboration Plan and will be submitted to the Collaboration Suppliers for approval.
  3. The Collaboration Suppliers will provide the help the Buyer needs to prepare the Detailed Collaboration Plan.
  4. The Collaboration Suppliers will, within 10 Working Days of receipt of the Detailed Collaboration Plan, either:
  5. approve the Detailed Collaboration Plan
  6. reject the Detailed Collaboration Plan, giving reasons for the rejection
  7. The Collaboration Suppliers may reject the Detailed Collaboration Plan under clause 3.4.2 only if it is not consistent with their Outline Collaboration Plan in that it imposes additional, more onerous, obligations on them.
  8. If the parties fail to agree the Detailed Collaboration Plan under clause 3.4, the dispute will be resolved using the Dispute Resolution Process.

## **4. Collaboration activities**

* 1. The Collaboration Suppliers will perform the Collaboration Activities and all other obligations of this Agreement in accordance with the Detailed Collaboration Plan.
  2. The Collaboration Suppliers will provide all additional cooperation and assistance as is reasonably required by the Buyer to ensure the continuous delivery of the services under the Call-Off Contract.
  3. The Collaboration Suppliers will ensure that their respective subcontractors provide all co-operation and assistance as set out in the Detailed Collaboration Plan.

## **5. Invoicing**

* 1. If any sums are due under this Agreement, the Collaboration Supplier responsible for paying the sum will pay within 30 Working Days of receipt of a valid invoice.
  2. Interest will be payable on any late payments under this Agreement under the Late Payment of Commercial Debts (Interest) Act 1998, as amended.

## **6. Confidentiality**

* 1. Without prejudice to the application of the Official Secrets Acts 1911 to 1989 to any Confidential Information, the Collaboration Suppliers acknowledge that any Confidential Information obtained from or relating to the Crown, its servants or agents is the property of the Crown.
  2. Each Collaboration Supplier warrants that:
  3. any person employed or engaged by it (in connection with this Agreement in the course of such employment or engagement) will only use Confidential Information for the purposes of this Agreement
  4. any person employed or engaged by it (in connection with this Agreement) will not disclose any Confidential Information to any third party without the prior written consent of the other party
  5. it will take all necessary precautions to ensure that all Confidential Information is treated as confidential and not disclosed (except as agreed) or used other than for the purposes of this Agreement by its employees, servants, agents or subcontractors
  6. neither it nor any person engaged by it, whether as a servant or a consultant or otherwise, will use the Confidential Information for the solicitation of business from the other or from the other party's servants or consultants or otherwise
  7. The provisions of clauses 6.1 and 6.2 will not apply to any information which is:
  8. or becomes public knowledge other than by breach of this clause 6
  9. in the possession of the receiving party without restriction in relation to disclosure before the date of receipt from the disclosing party
  10. received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure
  11. independently developed without access to the Confidential Information
  12. required to be disclosed by law or by any judicial, arbitral, regulatory or other authority of competent jurisdiction
  13. The Buyer’s right, obligations and liabilities in relation to using and disclosing any Collaboration Supplier’s Confidential Information provided under this Agreement and the Collaboration Supplier’s right, obligations and liabilities in relation to using and disclosing any of the Buyer’s Confidential Information provided under this Agreement, will be as set out in the [relevant contract] [Call-Off Contract].

## **7. Warranties**

* 1. Each Collaboration Supplier warrant and represent that:
  2. it has full capacity and authority and all necessary consents (including but not limited to, if its processes require, the consent of its parent company) to enter into and to perform this Agreement and that this Agreement is executed by an authorised representative of the Collaboration Supplier
  3. its obligations will be performed by appropriately experienced, qualified and trained personnel with all due skill, care and diligence including but not limited to good industry practice and (without limiting the generality of this clause 7) in accordance with its own established internal processes
  4. Except as expressly stated in this Agreement, all warranties and conditions, whether express or implied by statute, common law or otherwise (including but not limited to fitness for purpose) are excluded to the extent permitted by law.

## **8. Limitation of liability**

* 1. None of the parties exclude or limit their liability for death or personal injury resulting from negligence, or for any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982.
  2. Nothing in this Agreement will exclude or limit the liability of any party for fraud or fraudulent misrepresentation.
  3. Subject always to clauses 8.1 and 8.2, the liability of the Buyer to any Collaboration Suppliers for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement (excluding Clause 6.4, which will be subject to the limitations of liability set out in the relevant Contract) will be limited to 100% of the annual charges.
  4. Subject always to clauses 8.1 and 8.2, the liability of each Collaboration Supplier for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement will be limited to [Buyer to specify].
  5. Subject always to clauses 8.1, 8.2 and 8.6 and except in respect of liability under clause 6 (excluding clause 6.4, which will be subject to the limitations of liability set out in the [relevant contract] [Call-Off Contract]), in no event will any party be liable to any other for:
  6. indirect loss or damage
  7. special loss or damage
  8. consequential loss or damage
  9. loss of profits (whether direct or indirect)
  10. loss of turnover (whether direct or indirect)
  11. loss of business opportunities (whether direct or indirect)
  12. damage to goodwill (whether direct or indirect)
  13. Subject always to clauses 8.1 and 8.2, the provisions of clause 8.5 will not be taken as limiting the right of the Buyer to among other things, recover as a direct loss any:
  14. additional operational or administrative costs and expenses arising from a Collaboration Supplier’s Default
  15. wasted expenditure or charges rendered unnecessary or incurred by the Buyer arising from a Collaboration Supplier's Default

## **9. Dispute resolution process**

* 1. All disputes between any of the parties arising out of or relating to this Agreement will be referred, by any party involved in the dispute, to the representatives of the parties specified in the Detailed Collaboration Plan.
  2. If the dispute cannot be resolved by the parties' representatives nominated under clause 9.1 within a maximum of 5 Working Days (or any other time agreed in writing by the parties) after it has been referred to them under clause 9.1, then except if a party seeks urgent injunctive relief, the parties will refer it to mediation under the process set out in clause 9.3 unless the Buyer considers (acting reasonably and considering any objections to mediation raised by the other parties) that the dispute is not suitable for resolution by mediation.
  3. The process for mediation and consequential provisions for mediation are:
  4. a neutral adviser or mediator will be chosen by agreement between the parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one party to the other parties to appoint a Mediator or if the Mediator agreed upon is unable or unwilling to act, any party will within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to the parties that he is unable or unwilling to act, apply to the Chairman of the Law Society to appoint a Mediator
  5. the parties will within 10 Working Days of the appointment of the Mediator meet to agree a programme for the exchange of all relevant information and the structure of the negotiations
  6. unless otherwise agreed by the parties in writing, all negotiations connected with the dispute and any settlement agreement relating to it will be conducted in confidence and without prejudice to the rights of the parties in any future proceedings
  7. if the parties reach agreement on the resolution of the dispute, the agreement will be put in writing and will be binding on the parties once it is signed by their authorised representatives
  8. failing agreement, any of the parties may invite the Mediator to provide a non-binding but informative opinion in writing. The opinion will be provided on a without prejudice basis and will not be used in evidence in any proceedings relating to this Agreement without the prior written consent of all the parties
  9. if the parties fail to reach agreement in the structured negotiations within 20 Working Days of the Mediator being appointed, or any longer period the parties agree on, then any dispute or difference between them may be referred to the courts
  10. The parties must continue to perform their respective obligations under this Agreement and under their respective Contracts pending the resolution of a dispute.

## **10. Termination and consequences of termination**

### Termination

* 1. The Buyer has the right to terminate this Agreement at any time by notice in writing to the Collaboration Suppliers whenever the Buyer has the right to terminate a Collaboration Supplier’s [respective contract] [Call-Off Contract].
  2. Failure by any of the Collaboration Suppliers to comply with their obligations under this Agreement will constitute a Default under their [relevant contract] [Call-Off Contract]. In this case, the Buyer also has the right to terminate by notice in writing the participation of any Collaboration Supplier to this Agreement and sever its name from the list of Collaboration Suppliers, so that this Agreement will continue to operate between the Buyer and the remaining Collaboration Suppliers.

### Consequences of termination

* 1. Subject to any other right or remedy of the parties, the Collaboration Suppliers and the Buyer will continue to comply with their respective obligations under the [contracts] [Call-Off Contracts] following the termination (however arising) of this Agreement.
  2. Except as expressly provided in this Agreement, termination of this Agreement will be without prejudice to any accrued rights and obligations under this Agreement.

## **11. General provisions**

### Force majeure

* 1. For the purposes of this Agreement, the expression “Force Majeure Event” will mean any cause affecting the performance by a party of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or Regulatory Bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to any party, the party's personnel or any other failure of a Subcontractor.
  2. Subject to the remaining provisions of this clause 11.1, any party to this Agreement may claim relief from liability for non-performance of its obligations to the extent this is due to a Force Majeure Event.
  3. A party cannot claim relief if the Force Majeure Event or its level of exposure to the event is attributable to its wilful act, neglect or failure to take reasonable precautions against the relevant Force Majeure Event.
  4. The affected party will immediately give the other parties written notice of the Force Majeure Event. The notification will include details of the Force Majeure Event together with evidence of its effect on the obligations of the affected party, and any action the affected party proposes to take to mitigate its effect.
  5. The affected party will notify the other parties in writing as soon as practicable after the Force Majeure Event ceases or no longer causes the affected party to be unable to comply with its obligations under this Agreement. Following the notification, this Agreement will continue to be performed on the terms existing immediately before the Force Majeure Event unless agreed otherwise in writing by the parties.

### Assignment and subcontracting

* 1. Subject to clause 11.2.2, the Collaboration Suppliers will not assign, transfer, novate, sub- license or declare a trust in respect of its rights under all or a part of this Agreement or the benefit or advantage without the prior written consent of the Buyer.
  2. Any subcontractors identified in the Detailed Collaboration Plan can perform those elements identified in the Detailed Collaboration Plan to be performed by the subcontractors.

### Notices

* 1. Any notices given under or in relation to this Agreement will be deemed to have been properly delivered if sent by recorded or registered post or by fax and will be deemed for the purposes of this Agreement to have been given or made at the time the letter would, in the ordinary course of post, be delivered or at the time shown on the sender's fax transmission report.
  2. For the purposes of clause 11.3.1, the address of each of the parties are those in the Detailed Collaboration Plan.

### Entire agreement

* 1. This Agreement, together with the documents and agreements referred to in it, constitutes the entire agreement and understanding between the parties in respect of the matters dealt with in it and supersedes any previous agreement between the Parties about this.
  2. Each of the parties agrees that in entering into this Agreement and the documents and agreements referred to in it does not rely on, and will have no remedy in respect of, any statement, representation, warranty or undertaking (whether negligently or innocently made) other than as expressly set out in this Agreement. The only remedy available to each party in respect of any statements, representation, warranty or understanding will be for breach of contract under the terms of this Agreement.
  3. Nothing in this clause 11.4 will exclude any liability for fraud.

### Rights of third parties

* 1. Nothing in this Agreement will grant any right or benefit to any person other than the parties or their respective successors in title or assignees, or entitle a third party to enforce any provision and the parties do not intend that any term of this Agreement should be enforceable by a third party by virtue of the Contracts (Rights of Third Parties) Act 1999.

### Severability

If any provision of this Agreement is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, that provision will be severed without effect to the remaining provisions. If a provision of this Agreement that is fundamental to the accomplishment of the purpose of this Agreement is held to any extent to be invalid, the parties will immediately commence good faith negotiations to remedy that invalidity.

### Variations

No purported amendment or variation of this Agreement or any provision of this Agreement will be effective unless it is made in writing by the parties.

### No waiver

The failure to exercise, or delay in exercising, a right, power or remedy provided by this Agreement or by law will not constitute a waiver of that right, power or remedy. If a party waives a breach of any provision of this Agreement this will not operate as a waiver of a subsequent breach of that provision, or as a waiver of a breach of any other provision.

### Governing law and jurisdiction

This Agreement will be governed by and construed in accordance with English law and without prejudice to the Dispute Resolution Process, each party agrees to submit to the exclusive jurisdiction of the courts of England and Wales.

Executed and delivered as an agreement by the parties or their duly authorised attorneys the day and year first above written.

**For and on behalf of the Buyer**

Signed by:

Full name (capitals):

Position:

Date:

**For and on behalf of the [Company name]**

Signed by:

Full name (capitals):

Position:

Date:

**For and on behalf of the [Company name]**

Signed by:

Full name (capitals):

Position:

Date:

**For and on behalf of the [Company name]**

Signed by:

Full name (capitals):

Position:

Date:

**For and on behalf of the [Company name]**

Signed by:

Full name (capitals):

Position:

Date:

**For and on behalf of the [Company name]**

Signed by:

Full name (capitals):

Position:

Date:

**For and on behalf of the [Company name]**

Signed by:

Full name (capitals):

Position:

Date:

Collaboration Agreement Schedule 1 - List of contracts

|  |  |  |
| --- | --- | --- |
| Collaboration supplier | Name/reference of contract | Effective date of contract |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

[Collaboration Agreement Schedule 2 - Outline collaboration plan]

## **Schedule 4 - Alternative clauses**

## **1. Introduction**

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

The Parties set out below agreed clarifications in relation to certain aspects of the Call-Off Contract:

1. The Buyer acknowledges that the Supplier and/or its subcontractors (as applicable) has a number of policies and procedures in place to determine the suitability of any Supplier Staff” and the Buyer confirms that it is satisfied with the scope of the Supplier’s vetting procedures and that it does not require the Supplier to conduct any further vetting.
2. The Buyer confirms that it has reviewed the Supplier and/or its subcontractors (as applicable) business continuity and disaster recovery plan and that they are sufficient to discharge the Supplier’s obligations under the Call-Off Contract.
3. The Parties agree that no Project Specific IPRs or software will be created or arise out of the performance by the Supplier and/or its subcontractors (as applicable) (or by a third party on behalf of the Supplier) of its obligations under this Call-Off Contract.
4. The Buyer acknowledges that any Buyer Personal Data held by the Supplier and/or its subcontractors (as applicable) or Buyer Data processed by the Supplier and/or its subcontractors (as applicable) is capable of being accessed directly by the Buyer through the relevant software solution.
5. By signing this Call-Off Contract the Buyer gives its prior written consent to the Supplier and/or its subcontractors (as applicable) for the transfer of Buyer Personal Data to the Sub-processors identified in Schedule 7 of this Call-Off Contract – only in relation to the delivery of this contract
6. The Buyer confirms that it is satisfied with the security and compliance measures put in place in relation to the Supplier and/or its subcontractors’ (as applicable) system.
7. The Parties agree that the Supplier and/or its subcontractors (as applicable) will use all reasonable endeavours to (i) preserve the integrity of Buyer Data processed by the Supplier and/or its subcontractors (as applicable) and (ii) prevent its corruption and loss.
8. The Parties agree that any software or SaaS provided by the Supplier subcontractors to the Buyer pursuant to this Call-Off Contract will not be suitable for publication as open source.
9. The Parties agree that if Malicious Software originates from the Buyer’s system that the Buyer will be responsible for any costs, losses, claims or liabilities which are attributable to or caused by the same.
10. If the Buyer incurs any Losses at any time from any claim of infringement or alleged infringement of a third party’s IPRs, the Buyer agrees to (a) give the Supplier notice of any such claim, (b) give the Supplier sole control of the defence and settlement of the claim and (c) provide the Supplier with all reasonable assistance in the defence or settlement of such claim.
11. The Supplier acknowledges the various standards, policies, principles, guidance and best practice recommendations that are set out in the Call-Off Contract and the Parties agree that the Supplier will use all reasonable endeavours to comply with these.
12. The Buyer acknowledges that the Supplier and/or its subcontractors (as applicable) has a range of existing policies, procedures and systems in place to manage risks to security (all available on [www.unit4.com/terms](http://www.unit4.com/terms)) and the Buyer confirms that these are sufficient to discharge the Supplier and/or its subcontractors (as applicable) obligations under the Call-Off Contract.
13. Should there be a breach of security of the Buyer Confidential Information, the Parties agree that the Supplier will use all reasonable endeavours to recover the Buyer Confidential Information.
14. The Parties agree that at the end of the Call-Off Contract Term that all software licences granted by the Supplier and all services provided by the Supplier to the Buyer will cease.
15. For the purposes of clauses 5.9 to 5.11 of the Framework Agreement, the Parties agree that the references to a “a change of Control” means a change of Control in relation to the Supplier and/or its subcontractors (as applicable) only and not to any other member of its group (including its parent).
16. The Parties agree that the Call-Off Contract Charges are Commercially Sensitive Information which form part of the Supplier and/or its subcontractors (as applicable) ‘s Confidential Information and as such, should the Buyer receive a FoIA request, the Buyer undertakes, to the extent permitted by law, to redact the Call-Off Contract Charges in any response to such a request.

## **2. Clauses selected**

None

## **Schedule 5 - Guarantee**

Not required

## **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** | 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:   1. (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time 2. (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to Processing of personal data and privacy; 3. (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 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:  <http://tools.hmrc.gov.uk/esi> |
| **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 RM1557.11 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** | The General Data Protection Regulation (Regulation (EU) 2016/679). |
| **Good Industry Practice** | Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances. |
| **Government Procurement Card** | The Government’s preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/government-procurement-card--2. |
| **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 applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body. |
| **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: pseudonymising 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**

The information below relates to Annex A(i) – Unit4 Agreement Regarding the Processing of Personal Data (“**DPA**”) a copy of which is available online at [www.unit4.com/terms](http://www.unit4.com/terms). These schedules apply when Customer enters into either (i) an Agreement under Appendix A of Unit4’s General Terms of Business or (ii) a DPA.

1. The PERSONAL Data that WILL BE processed:

|  |  |  |
| --- | --- | --- |
| Product | Personal Data that may be processed might include: | To whom this may belong: |
| Unit4 Business World | Names; addresses; contract details; telephone numbers (including mobile); email address(es); other contact information; date of birth; age; place of birth; nationality or citizenship; residency; domicile; spoken language(s); passport number; national security number or social security number or ID card reference; marital status; beneficiary details under benefits; gender; employment information (including: salary; position; pay scale; pay step; competences and personal notes); tax information; benefits information; union membership; next of kin provided (name; address; birthdate; phone number; emergency contact details); start and end dates of employment; bank account or credit card details; personal service company details (name; registration number and registered office); directorships; VAT numbers; documents (written or electronic) containing any of the above. | * Current or former employees; * Contractors or Sub-contractors (of any variety), agents or directors; and * Applicants or prospective employees. |
| Unit4 Financials | Names; addresses; contract details; telephone numbers (including mobile); email address(es); other contact information; date of birth; age; place of birth; nationality or citizenship; residency; domicile; spoken language(s); passport number; national security number or social security number or ID card reference; marital status; beneficiary details under benefits; gender; employment information (including: salary; position; pay scale; pay step; competences and personal notes); tax information; benefits information; union membership; next of kin provided (name; address; birthdate; phone number; emergency contact details); start and end dates of employment; bank account or credit card details; personal service company details (name; registration number and registered office); directorships; VAT numbers; documents (written or electronic) containing any of the above. | * Current or former employees; * Contractors or Sub-contractors (of any variety), agents or directors; and * Applicants or prospective employees. |
| Unit4 Student Management | Names; addresses; contract details; telephone numbers (including mobile); email address(es); other contact information; date of birth; age; place of birth; nationality or citizenship; residency; domicile; spoken language(s); passport number; national security number or social security number or ID card reference; marital status; beneficiary details under benefits; gender; employment information (including: salary; position; pay scale; pay step; competences and personal notes); tax information; benefits information; union membership; next of kin provided (name; address; birthdate; phone number; emergency contact details); start and end dates of employment; bank account or credit card details; personal service company details (name; registration number and registered office); directorships; VAT numbers; documents (written or electronic) containing any of the above.  Additional Personal Data for former and current employees: staff type (e.g. faculty, advisor, housing director); academic department; hire status; employment status; workload; faculty rank; publications; work status tracking; education details and qualification details.  Additional Personal Data for former and current applicants: prior college information; transscripts and/or (additional) test results; physical health status; former employer letters; and workplace information.  Additional Personal Data for former and current students: academic record including results and goals; enrolment details; academic progression details (including grades); academic achievements; work or academic placements; course planning details; billing and payment history; housing preferences and history; financial aid details; health record (including vaccinations, allergies, medical conditions), insurance information and health documentation. | * Current or former employees (including any faculty or personnel); * Contractors or Sub-contractors (of any variety), agents or directors; * Applicants or prospective employees; and * Current, former and prospective students. |
| Unit4 prevero | Names; addresses; telephone numbers (including mobile); email address(es); other contact information. Other Personal Data is not required to be stored or processed to achieve the objectives of the Product (as set out below), but other Personal Data may be stored or processed by the Product if it is configured in such a way to do so (e.g. salary data) or is inputted into the Product by the Customer. | * Current or former employees; * Sub-contractors (of any variety), agents or directors. |
| Unit4 Assistance PSA Suite | Names; addresses; telephone numbers (including mobile); email address(es); other contact information. Other Personal Data is not required to be stored or processed to achieve the objectives of the Product (as set out below), but other Personal Data may be stored or processed by the Product if it is configured in such a way to do so or is inputted into the Product by the Customer. | * Current or former employees; * Sub-contractors (of any variety), agents or directors; * Anyone else who is a member of a project team (including non-employees) * applicants or prospective employees. * Customer’s customer contacts and supplier contacts. |
| People Platform Services (“**PPS**”) (generally) including IDS and Wanda (together with any supporting services) | As the PPS are services that work and interface with Unit4’s other Products or Services, they may process any or all types of Personal Data set out in this table in relation to the listed Products and Services.  Additionally, Wanda may process: Unit4Id (which identifies the user of IDS); any Personal Data or information submitted by the user into an application to which Wanda may be connected (such information being processed or stored unless User elects to have it deleted); any other conversation and dialog data; metadata where assignable to an individual; and Application Insights Logs (a Microsoft service utilised for performing diagnostics). | All categories of individual listed in this table.  Depending on the application or service to which Wanda is connected, the PPS could potentially Process Personal Data relating to any living individual that the User chooses to submit. |

1. NATURE AND OBJECTIVE(S) of PROCESSING:

Generally, the nature of the Processing by the Processor will only be as is necessary to enable the Processor to comply with its obligations and exercise its rights under the Master Agreement, including (in relation to the Personal Data) collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. The objective or purpose of the Processing is the performance of the Processors obligations and exercise of its rights under this DPA, including the performance of functions required or requested by the Data Controller for the Data Controller’s compliance with its statutory and/or contractual obligations. In relation to and depending on the Product or Service, Processing will include the following:

|  |  |
| --- | --- |
| Product | Nature and Objective of Processing |
| Unit4 Business World | Personal Data will be entered into Unit4 Business World to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include:   * Travel requests; * Expense claim processing; * Timesheet processing; * Absence management; * HR & Payroll related processes:   + Payroll;   + Course enrolment;   + Competence management;   + Appraisals;   + Salary review;   + Applicant registration; * Payment processing; * Billing; * Purchase requisitions; * People/Project Planning.     The Processing will involve:  ***Product (software solution)***   * Unit4 Business World executing programmable software code to provide that the activities set out (above) are able take place. This may involve transferring data to or from Third Party solutions not under the control of the Processor through integrations.   ***Services***   * Transfer and storage of Personal Data to provide additional Unit4 Global Cloud Services as set out in more detail in the Unit4 Global Cloud Service Description or People Platform Services (as set out in the applicable People Platform Service Service Description). * Access to the Personal Data to provide support and maintenance of the Unit4 Business World Product and assist the Customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. * Access to the Personal Data to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer. |
| Unit4 Financials | Personal Data will be entered into Unit4 Financials to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include:   * Customer/Supplier/Employee registration; * Payment processing; * Billing; * Expense claim processing; * Travel requests; * Purchase requisitions & Orders; * People/Project Planning; * HR & Payroll related processes:   + Payroll;   + Timesheet processing;   + Absence management   + Course enrolment;   + Competence management;   + Appraisals;   + Salary review;   + Applicant registration;   The Processing will involve:  **Product (software solution)**   * Unit4 Financials executing programmable software code to provide that the activities set out (as detailed above) are able take place. This may involve transferring data to or from Third Party solutions not under the control of the Processor through integrations.   **Services**   * Transfer and storage of Personal Data to provide additional Unit4 Global Cloud Services as set out in more detail in the Unit4 Global Cloud Service Description or People Platform Services (as set out in the applicable People Platform Service Service Description). * Access to the Personal Data to provide support and maintenance of the Unit4 Financials Product and assist the customer in the operation of the solution as set out in more detail in the Unit4 Support Terms * Access to the Personal Data in order to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer. |
| Unit4 Student Management | Personal Data will be entered into Unit4 Student Management to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include:   * Recruiting prospective students, * Responding to information requests * Processing applications * Managing the academic lifecycle of a student including onboarding, course scheduling, academic progression, advisory, housing and other facilities, graduation * Planning and scheduling faculty staff   The Processing will involve:  **Product (software solution)**   * Unit4 Student Management executing programmable software code to provide that the activities set out (above) are able take place. This may involve transferring data to or from Third Party solutions not under the control of the Processor through integrations.   **Services**   * Transfer and storage of Personal Data to provide additional Unit4 Global Cloud Services as set out in more detail in the Unit4 Global Cloud Service Description or People Platform Services (as set out in the applicable People Platform Service Service Description). * Access to the Personal Data to provide support and maintenance of the Unit4 Student Management Product and assist the customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. * Access to the Personal Data in order to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer. |
| Unit4 prevero | Personal Data will be entered into Unit4 prevero to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include:   * Budgeting; * Financial and other reporting; * Report distribution; * Approval processing; * People/Project planning.   The Processing will involve:  **Product (software solution)**   * Unit4 prevero executing programmable software code to provide that the activities set out (above) are able take place. This may involve transferring data to or from Third Party solutions not under the control of the Processor through integrations.   **Services**   * Transfer and storage of Personal Data to provide additional Unit4 Global Cloud Services as set out in more detail in the Unit4 Global Cloud Service Description or People Platform Services (as set out in the applicable People Platform Service Service Description). * Access to the Personal Data to provide support and maintenance of the Unit4 prevero Product and assist the Customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. * Access to the Personal Data to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer. |
| Unit4 Assistance PSA Suite | Personal Data will be entered into Unit4 Assistance PSA Suite to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include:   * automation of a professional services organization, including financial and human resource management (HRM); * daily time and project management; * booking time and expenses with receipts; * transitioning opportunities into projects, budget and forecasting hours and planning projects and resources; * tracking time and expenses and execute invoicing; * integration of projects into other applications * performing accounting assisting the integration of financial data into other solutions.   The Processing will involve:  **Product (software solution)**   * Unit4 Assistance PSA Suite executing programmable software code to provide that the activities set out (as detailed above) are able take place. This may involve transferring data to or from Third Party solutions not under the control of the Processor through integrations.   **Services**   * Transfer and storage of Personal Data to provide additional Unit4 Global Cloud Services as set out in more detail in the Unit4 Global Cloud Service Description or People Platform Services (as set out in the applicable People Platform Service Service Description). * Access to the Personal Data to provide support and maintenance of the Unit4 Assistance PSA Suite Product and assist the Customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. * Access to the Personal Data in order to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer. |
| People Platform Services (“**PPS**”) (generally) including IDS and Wanda (together with any supporting services) | Data will be processed by the PPS to permit the stated purposes of the services as set out in the applicable Appendix G - Service Description on [www.unit4.com/terms](http://www.unit4.com/terms).  In addition, Personal Data will be inputted into Wanda using third party software of choice (e.g. Slack Integration, Facebook Messenger or other Microsoft Applications (including Microsoft Teams)). Dependent on the Unit4 Product or Service used by Customer, Wanda can help to complete administrative tasks for Customer’s employees.  Tasks may include:   * Timesheet entries * Expense entries * Travel requests * Payslip enquiries * Absence entries * Balance enquiries * Purchase requisitions.     The Processing will involve:  ***Product (software solution)***   * Wanda executing programmable software code to provide that the activities set out (above) are able take place. This may involve transferring data to or from Third Party solutions not under the control of the Processor through integrations.   ***Services***   * Transfer and storage of Personal Data to provide additional Unit4 Global Cloud Services as set out in more detail in the Unit4 Global Cloud Service Description or People Platform Services (as set out in the applicable People Platform Service Service Description). * Access to the Personal Data to provide support and maintenance of the Unit4 PPS and assist the Customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. * Access to the Personal Data in order to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer. * Access to Personal Data for product improvement via AI machine learning or data analysis. |

1. Description of the processing and means:

Processor will Process the aforementioned Personal Data in connection with the following activities (the activities below are mentioned as example only):

|  |  |  |
| --- | --- | --- |
| Type of Processing | Description | Means and resources |
| Global Cloud Services (Unit4 SaaS or Unit4 Managed Cloud) | The Processor will Process Personal Data in connection with the activities as described in the Master Agreement and more specifically the Unit4 Global Cloud Services Description and Solution Specific Service descriptions. | Personnel  The Unit4 Global Cloud Services operations team has personnel in Poland, Sweden, Norway, UK, US, Canada, Malaysia and Singapore. These Processor personnel operate the Unit4 Global Cloud Services.  Assets and Infrastructure  Unit4 utilises third party hosting infrastructure services to provide the Unit4 Global Cloud Services and employs other software systems for operation and management. See Schedule 4. |
| Support Services | The Processor will Process Personal Data in connection with the activities as described in the Master Agreement and more specifically in the Unit4 Support Terms. | Personnel  The Unit4 Support team has personnel in these locations United Kingdom, Poland, Portugal, Norway, Germany, Sweden, Germany, US, Canada (and such other locations as required to support the Unit4’s business needs). These Processor personnel provide the Unit4 Support Services (set out in the Unit4 Support Terms in Section B of the SLA).  Assets and Infrastructure  Unit4 utilises other software systems for operation, delivery and management of these services. |
| Professional Services and/or consulting | The Processor will Process Personal Data in connection with the activities as described in the Master Agreement and more specifically in any more detailed Project documentation or statements of work agreed between the Parties following Project commencement. | Personnel  The Unit4 Professional Services team has personnel in all locations where Unit4 has a corporate group entity including United Kingdom, Ireland Poland, Portugal, Norway, Spain, France, Germany Sweden, US, Canada, Singapore/Malaysia (and such other locations as required to support Unit4’s business needs). These Processor personnel provide the Unit4 Professional Services.  Assets and Infrastructure  Unit4 utilises other software systems for operation, delivery and management of these services. |
| Unit4 Professional Services (if sub-contracted to a delivery partner) | The Processor and its sub-processors will Process the aforementioned Personal Data in connection with the activities as described in the Master Agreement and (if any) the Third Party contractual and service documentation provided as part of the Master Agreement. For more details, See Schedule 4.  The Processor will execute a written agreement with the Sub-processor(s), which will be in accordance with the relevant legislation and regulations and this DPA.  Further, the Data Controller has given the Processor permission to engage the applicable Sub-processor(s) as listed in Schedule 4 by signing this DPA. | See Schedule 4. |
| Third Party Products and Services | The Processor and its sub-processors will Process the aforementioned Personal Data in connection with the activities as described in the Master Agreement and the Third Party contractual and service documentation provided as part of the Master Agreement. | See Schedule 4 and any additional provisions provided in further schedules or appendices to this DPA if required by the Third Party Provider or Applicable Law. |
| People Platform Services (“**PPS**”) (generally) including IDS and Wanda (together with any supporting services) | In addition to the “Global Cloud Services”, the PPS will (where applicable) process Personal Data in connection with a privacy statement as presented to the end user, asking for consent, where such Personal Data is processed. | Personnel  The Unit4 Global Cloud Services operations team, which operates the PPS, has personnel in Poland, Sweden, Norway, UK, US, Canada, Malaysia and Singapore. These Processor personnel operate the Unit4 Global Cloud Services.  Assets and Infrastructure  Unit4 utilises its own and third party (shared) infrastructure services to provide the Unit4 People Platform services. This includes 3rd party systems (i.e. collaboration apps), over which Unit4 has no control. The PPS including Wanda make use of a number of Microsoft products and services, as follows:   * Cognitive services:   + LUIS Cognitive Service - *language understanding.*   + Text Translator API – *translating text*   + QnA Maker Cognitive service – *provides a questions and answers service* * Bot framework connectors – *provides for the connection of Wanda to the supported social channels*. * Traffic manager – *used for disaster recovery and failover if the primary region is unhealthy* * Web apps / web jobs – *hosts web APIs and long running web-based processes* * Service bus *– provides internal communication in the Wanda ecosystem* * Storage accounts – *used to store conversation state and user settings* * Cosmos DB *–provides storage* * Key vault *– stores confidential data that is used to communicate with Microsoft services and for internal services* * Redis cache – *provides caching capabilities* * Application Insights – *Monitoring of system, includes telemetry and logging* * *SQL server – provides storage* * Kubernetes *– open source container*   Further information and details relating to those Microsoft products and services can be found here: <https://azure.microsoft.com/en-us/services/>. |

1. Retention period

The Processor will keep the Personal Data for the duration of the Master Agreement.

After the agreed period of retention, the Processor will return the Personal Data to the Data Controller, on a migration-capable format set by Processor **or** immediately destroy the Personal Data without retaining a copy, upon first request of Data Controller.

1. INFORMATION REGARDING COUNTRY (OR PLACE) OF PROCESSING OF PERSONAL DATA

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Product - On premises | Data is stored on the servers of the Data Controller in their principal place of business or registered office as can be notified to Unit4 from time to time. | | | | |
| Product - Unit4 Global Cloud Services | Unit4 Global Cloud operates in several data centres, including a worldwide presence in Microsoft Azure. Unit4 will deploy the customer in the most logical location dependent on where the Customer resides (as set out in an Order Form). All Customer data will be stored only in the selected geo-political zone and won’t be moved outside of it without explicit customer consent. | | | | |
| Cloud Model | GEO-POLICITAL Zone | Location OF DATA CENTRE | | Facility or Partnership |
| Managed Cloud | Benelux | Amsterdam / Ede | | Digital Reality / Bit |
| Managed Cloud | Sweden | Stockholm | | Sungard |
| Managed Cloud | UK (Wales) | Newport | | NGD |
| Managed Cloud | UK (England) | London | | Digital Reality |
| Managed Cloud | US | Multiple locations | | Amazon Web Services (AWS) |
| Managed Cloud | Canada | Toronto | | IBM Softlayer |
| SaaS/Managed Cloud | EU | Dublin / Amsterdam | | Microsoft Azure |
| SaaS/Managed Cloud | USA | Multiple locations | | Microsoft Azure |
| SaaS/Managed Cloud | Canada | Toronto / Quebec City | | Microsoft Azure |
| SaaS/Managed Cloud | United Kingdom | London / Cardiff | | Microsoft Azure |
| SaaS/Managed Cloud | Asia | Singapore / Hong Kong | | Microsoft Azure |
| SaaS/Managed Cloud | Australia | Victoria / New South Wales | | Microsoft Azure |
| Unit4 Support – Standard Support and other standard support services | Unit4 Support uses SalesForce to register and process Cases. These Cases are accessible for any Unit4 employee that is provided access to SalesForce such as support engineers, cloud engineers, Professional Services consultants and service management. Access is controlled by internal management and organisational processes, to ensure that Personal Data is not accessed by consultants or engineers in locations that should not have access to particular Customer details. | | | | |
| Customer Location | | Primarily Support is provided from: | | |
| United Kingdom and Ireland | | United Kingdom, Ireland, Portugal and Poland. | | |
| Sweden, Norway, Denmark, Finland and Iceland | | Poland, Portugal, Norway and Sweden. | | |
| US & Canada | | Poland, Portugal, US and Canada. | | |
| Europe rest | | Poland, Portugal and Germany. | | |
| APAC | | Poland, Portugal and Singapore/ Malaysia. | | |
| Unit4 Support – 24/7 Support  (Enhanced and Premium Support Customers) | Using a ‘follow the sun’ methodology, 24/7 support of Customer Cases could occur in any of the support locations listed above. | | | | |
| Unit4 Support – EU Only Support | If EU Only support is elected, Cases are supported only within the EU locations listed above for standard support (during Business Hours). | | | | |
| People platform services (“PPS”) (generally) including IDS and Wanda (together with any supporting services) | PPS are cloud services that use shared infrastructure and 3rd party services that might not provide geopolitical zone isolation. Below is an overview of the PPS and the country (or place) of Processing of Personal Data using that service. | | | | |
| Service | Geo-political zone | Where Service Processes or Stores Data | Primarily Support is provided from: | |
| Wanda | Any | Predominantly within the EU, but may be elsewhere. | Ireland, United States and other Global support where required | |
| IDS | Depends on Cloud Deployment | As above for Global Cloud Service | As above for Global Cloud Service | |
| Unit4 Professional Services and Unit4 customer success function | Topic | Professional Services and customer success are provided from: | | | |
| Implementation and other project services | In the Territory or Customer location of registered office/principal place of business (as applicable) and/or Portugal depending on what is agreed between the Parties in the project documentation or a statement of work (if applicable). | | | |
| Data Migration | In the Territory or Customer location of registered office/principal place of business (as applicable) and/or Portugal depending on what is agreed between the Parties in the project documentation or a statement of work (if applicable). | | | |
| Trouble shooting | In applicable Unit4 Support Service location and Portugal. | | | |
| Customer Success | In applicable Unit4 Support Service location and Portugal. | | | |

1. CONTACT DETAILS

For questions or comments about the DPA and Schedules the contact person is  
  
Data Processor: By letter (addressed to Global Data Privacy Officer copy to Corporate Legal Department) P.O. Box 5005, 3528 BJ Utrecht, the Netherlands or by email to [privacy@unit4.com](mailto:privacy@unit4.com) or to the Unit4 address for notices provided in the Master Agreement.

Controller: The Data Controller address for notices provided in the DPA or Master Agreement.

SECURITY MEASURES

As stated in article 7 of the DPA, the technical and organisational security measures are listed in this schedule and are supplemented or amended if necessary. The Data Controller considers these measures suitable for the processing of Personal Data.

**Unit4 Business Security Measures (Internal business operations summary)**

Description of the technical and organisational security measures implemented by the Processor in its organisation (generally):

***Physical Security:***

* Physical access control is managed by Unit4 facilities.
* All offices have security systems in place in respect of controlling access through barriers, e.g. entry gates, manned reception desks, alarmed fire doors, intruder detection systems and lockable offices.
* Unit4 operates access controls with the help of what people know, such as password or personal access code; or with the help of what people carry, such as a security pass;
* On-site server rooms (where applicable) have additional physical controls.
* Access to secure areas or sensitive information is restricted to prevent unauthorized access by visitors / unauthorized staff (by way of lockable offices or lockable cabinets) and operating clear desk policies where appropriate.
* Unit4 visitors are controlled at reception (whether by a dedicated receptionist or other member of staff).
* Shredders or other suitable secure disposal method for sensitive documents are used.

***Virtual and computing Security:***

* The responsible line manager will ensure employees and contractors return all Unit4 assets in their possession upon termination of their employment or contract agreement.  Records of this return of asset are maintained in the ticketing system.
* Unit4 aims to classify information as either public, confidential, proprietary or sensitive. Information would then be protected according to its classification.
* Media (including hard drives) are disposed of securely and safely when no longer required. All sensitive material (hard disks, floppies, etc.) is removed by guaranteed removal software, (not by reformatting or deletion) before disposal or physical destruction.
* Anti-malware - we use the latest version of industry standard solutions to provide virus and anti-malware protection.
* Further, Unit4 utilises:
  + control on assigned rights;
  + logging and controlling access to the system;
  + recovery measures;
  + the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; and
  + systems and processes to allow it to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
* Business Continuity and Disaster Recovery plans have been prepared which include information security considerations.

***Security Policies and Documentation:***

* The Global Leadership Team for Unit4 and/or its respective local management teams have oversight of both global and local information management and security plans including any information security policies that meet identified information security risks and supports the business goals.
* Information security and management is assigned globally to the Global Information Security Manager and Global Data Privacy Officer, who manage resources to deliver strategic and overall compliance with information security policy and process.
* Unit4 has implemented security policies updated and amended regularly to comply with good industry practice.
* Unit4 has a privacy policy and white paper on GDPR published on [www.unit4.com/about/ethics](http://www.unit4.com/about/ethics).
* Unit4 enters into non-disclosure and confidentiality agreements with Third Parties when sharing confidential information relation to its business.
* Unit4 ensures all employees and contractors enter into standard confidentiality clauses in their contracts.
* Unit4 provides all employees with training in relation to: data protection; security and its core business principles as stated above.

**Additional Elements for Unit4 Global Cloud Services on Microsoft Azure (summary)**

Description of the technical and organisational security measures implemented by the Processor in relation to the provision of the Unit4 Global Cloud Services:

**Data protection**

Unit4 Global Cloud utilizes several mechanisms to protect personal data in the cloud. Below is a comprehensive overview of applied controls.

Network level security features, process and protocols

* Secure data transmission over public networks – all traffic is secured using industry standard protocols such as SSL/TLS and HTTPS.
* System security – Logical authentication and authorization mechanism in place
* Firewalls – next generation firewall technology to ensure inbound and outbound traffic is controlled.

Database level security features, process and protocols

* Data security – Logical authentication and authorization mechanism in place.
* Database security – Every customer has their own secure database which means partitioning of databases is not required and customer data not co-mingled. The outcome is that a customer’s data is never inadvertently shared with others.
* Backups are encrypted using whole database encryption technology such as Transparent Database Encryption. Azure Storage Service Encryption to encrypt all data placed into a customer’s storage account.
* Unit4 uses Azure Key Vault to maintain control of keys used by cloud applications and services to encrypt data.

Continually tested and evolving security

To uncover unforeseen vulnerabilities and refine our detection and response capabilities, we are continually looking into how we can improve out security posture to defend against potential breaches. The Unit4 Global Cloud operations team that closely monitor and secures Unit4’s Global Cloud operations (cloud infrastructure, cloud services, products, devices and internal resources) — testing penetration and improving our ability to protect, detect and recover from cyber threats.

Threat detection, mitigation and response

As the number, variety and severity of cyber threats have increased, so has our diligence in threat detection and response. Centralized monitoring systems provide continuous visibility and timely alerts. Frequent application of security patches and updates helps protect systems from known vulnerabilities. Intrusion and malware detection systems are designed to detect and mitigate risks from outside attacks. In the event of malicious activity, our incident response team follows established procedures for incident management, communication and recovery. The team uses industry best practices to alert both internal teams and customers. Finally, security reports monitor access patterns to help proactively identify and mitigate potential threats.

Data segregation

Data is the currency of the digital economy and we take the responsibility of protecting customer data very seriously. Both technological safeguards, such as encrypted communications and operational processes help keep customer data secured. In the Cloud, data from multiple customers may be stored on the same IT resources. Unit4 uses logical isolation to segregate each customer’s data from that of others. Unit4 SaaS is designed to counter risks inherent in a multitenant environment. Data storage and processing is logically separated among consumers using for instance Dedicated Accounts and having separate database instances for all our customers.

Network isolation at several points:

* Each dedicated deployment is isolated from other deployments and communicate through private IP addresses.
* Customer VMs can only communicate with other VMs owned or controlled by the same Customer and with infrastructure service endpoints meant for public communications.
* Traffic between VMs always traverses through trusted packet filters.

More details about the Security Policy and Security Program can be found at [www.unit4.com/terms](http://www.unit4.com/terms).

**Data encryption**

Unit4 provides, as a standard, secure access to all its services by encrypting all data in transit traveling on public networks. This is done by using only secure protocols, like HTTPS over TLS, using latest security ciphers. Encryption of data at rest can be optionally ordered by the customers. The mechanism used is a transparent, whole database encryption – TDE. Microsoft Azure customers in the Public SaaS offering get the TDE data at rest encryption as a standard.

**Access control**

Customers using Unit4 products in the Cloud are fully empowered to conduct front-end access control to their application. This means that the responsibility for creating new accounts, account termination and review for Unit4 application is with the customer.

Unit4 will retain limited back-end access to customer data (by direct database connection). Access by Unit4 to personal information shall be strictly limited to activities necessary for installing, implementing, maintaining, repairing, troubleshooting or upgrading the solution. All access is logged and limited to a small group of Cloud Engineers and Support Consultants. Access logs are saved in the centralized monitoring solution for 365 days. In case of data breaches, Unit4 can provide the access log on request.

**Data breach notification**

Unit4 shall notify the Customer without undue delay after becoming aware of a data breach. Customer should make sure that the contacts listed in Unit4 Support Portal are always up to date, as they will be used for all communication.

**Data privacy and security by design**

Unit4 Cloud platform was designed from the ground up with data security and privacy in mind. Unit4 is continually improving the security of the solution, by applying lessons learned from annual penetration tests and audits.

As a proof of secure design and operations, Unit4 Global Cloud Services SaaS Ops holds ISO 27001:2013 certification and ISAE3402 (SOC1) report. Unit4 and the data centres operators hold various security certifications, for the details please refer to the Global Cloud Service Description.

**Additional Elements for Unit4 People Platform Services (summary)**

Description of the technical and organisational security measures implemented by the Processor in relation to the provision of the Unit4 People Platform Services (Cloud only):

**Data protection**

Unit4 People Platform utilizes several mechanisms to protect personal data in the cloud. Below is a comprehensive overview of applied controls.

Network level security features, process and protocols

* Secure data transmission over public networks – all traffic is secured using industry standard protocols such as SSL/TLS (1.2) and HTTPS.

Authentication

* All services follow the principle of least privilege and authentication towards services and their APIs are secured using industry standard mechanisms. OpenID Connect and the underlying oAuth 2.0 protocol is used to securely perform authentication of users and/or client services with trusted parties and validate identity and access using claims based tokens.
* HMAC (Hash-based Message Authentication) is used as alternative method to secure communication between services.

Database level security features, process and protocols.

* A data stored in storage accounts are encrypted at rest.
* All storage accounts require secure transfer – all traffic is secured using industry standard protocols such as SSL/TLS and HTTPS.
* All data stored in Azure Cosmos DB is encrypted at rest and in transport.
* All Azure SQL Servers are enabled with Transparent Data Encryption (TDE).
* All Azure SQL Servers are running with Threat detection and auditing enabled.
* Azure KeyVault is used to secure particular sensitive information like service principal credentials.

Messaging level security features, process and protocols.

* All data stored by Azure Service Bus instances are encrypted at rest.
* All traffic (in transit) on the Azure Service Bus is secured using industry standard protocols such as SSL

More details about the Security Policy and Security Program can be found at [www.unit4.com/terms](http://www.unit4.com/terms).

**Data encryption**

Unit4 People Platform services provide, as a standard, secure access to all its services by encrypting all data in transit traveling on public networks. This is done by using only secure protocols, like HTTPS over TLS (1.2), using latest security ciphers. All data stored are encrypted.

**Data breach notification**

Unit4 shall notify the Customer without undue delay after becoming aware of a data breach. Customer should make sure that the contacts listed in Unit4 Support Portal are always up to date, as they will be used for all communication.

**Data privacy and security by design**

Unit4 People Platform services were designed from the ground up with data security and privacy in mind. Unit4 is continually improving the security of the solution, by applying lessons learned from annual penetration tests and audits.

SUB-PROCESSORS

|  |  |  |  |
| --- | --- | --- | --- |
| **Service** | **Sub-processor**  (company name, location etc.) | **Processing location** | **Type of service by**  **Sub-processor** |
| Unit4 Professional Services (if sub-contracted to a delivery partner) | As specified in the Master Agreement. | As specified in the Master Agreement. | As specified in Order Form or agreed in writing with Customer. |
| Third Party Products and Services only applicable when purchased by customer | As specified in the Master Agreement. | As provided in the Master Agreement or in any further schedules or appendices to the Agreement relating to the Third Party Provider processing. | Software and//or Support Services and/or Cloud Services. |
| Unit4 Global Cloud Services | Microsoft Azure | As stated above in Schedule 2, paragraph 5. | Providing Cloud Infrastructure and Services |
| Microsoft Dynamics | As stated above in Schedule 2, paragraph 5. | Providing Software Services, in particularly Microsoft Dynamics (including some cloud infrastructure). |
| Microsoft | As stated above in Schedule 2, paragraph 5. | Providing software tooling and Office |
| Sungard | As stated above in Schedule 2, paragraph 5. | Providing Cloud Infrastructure and Services |
| Digital Realty | As stated above in Schedule 2, paragraph 5. | Providing Cloud Infrastructure and Services |
| Amazon Web Services | As stated above in Schedule 2, paragraph 5. | Providing Cloud Infrastructure and Services |
| Bit Data Center | As stated above in Schedule 2, paragraph 5. | Providing Cloud Infrastructure and Services |
| IBM Softlayer | As stated above in Schedule 2, paragraph 5. | Providing Cloud Infrastructure and Services |
| NGD | As stated above in Schedule 2, paragraph 5. | Providing Cloud Infrastructure and Services |
| People Platform Services (“**PPS**”) (generally) including IDS and Wanda (together with any supporting services) | Microsoft Azure | As stated above in Schedule 2, paragraph 5 and as provided by Microsoft here: <https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located>. | Providing Cloud Infrastructure and platform Services (as set out above) in Section 2. |

# 

## **Schedule 8 – Software**

### Software List:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Date** |  |
| **Unit4 Business World Software Checklist** |  | **Prospect** | **The Insolvency Service** |
| **Product Engine (Expand to see detail of each Engine)** |  | **Required Y/N** | **Notes** |
| **Core Engine** |  | **Y** |  |
| Workflow Common (CM), Flexi Fields (AFF), Forms (FS), Reporting and Analysis Suite (XRS), Report viewing (WRP), IntellAgent (XIP), Analyser (In-Memory) (IAN), Experience Pack Modeller (XCR01), Dates on Relations Activation (DOR), Experience Pack Tasks (XT101), Collaboration (XIC01), Experience Pack Timelines (XTL01), Workflow on Reporting output (WR) |  |  |  |
| **Tuning Engine** |  | **Y** |  |
| Web services (WCS) |  |  |  |
| **Accounting** |  | **Y** |  |
| Financial Information Centre (IIK), General Ledger (FGL), Workflow Financials (WFF), Fixed Assets (FAT), Bank Reconciliation (FCB), Accounts Payable (FSU), Commitment Accounting (CO), Contract Accounting (FCN), Accounts Receivable (FCU), Cash Accounting (FCA), Sales Orders (LSO), Utility Invoicing (LUI), Planner (FPL)  \* |  |  | Cash Accounting Not Required |
| **Procurement** |  | **Y** |  |
| Purchasing (LPO), Workflow Procurement (with requisitioning) (WFL), Inventory Management (LST) |  |  |  |
| **Projects** |  | **Y** |  |
| Project Core (PTS), Workflow Project (WFP), Project Invoicing (PPI), Experience Pack People Planner (XRS10), Experience Pack Project Planner (XRS20) |  |  |  |
| **Core HR** |  | **Y** | Required for RTI interface for redundancy payments not licensed for Human Resources. |
| Human Resources (HPS), Workflow Human Resources (WFHR), Training Administration (HTA), Competences (HCV), Experience Pack Absences (XPS01), Absence (HPA), Expense Ledger (HTT), Experience pack Expenses (XTT01), Travel Expenses (WTR) |  |  | Note expenses are included as per notes below and any dependent modules |
| **Payroll** |  | Y | Required for RTI interface for redundancy payments – not licensed for Payroll |
| Payroll (HPR), Position register (payroll) (HP2), Salary Review (HPN) |  |  |  |
| **Field Service** |  | **N** |  |
| **Vertical Engines** |  | **N** |  |
| **Real Estate** |  | **N** |  |
| **Wholesale** |  | **N** |  |
| **Research** |  | **N** |  |
| **Education** |  | **N** |  |
|  |  |  |  |
| **Confirm modules required for User Numbers** | | **Required Y/N** | **Notes** |
| Report Viewing, Information pages |  | **Y** |  |
| Alerts |  | **Y** |  |
| Collaboration |  | **Y** |  |
| In-Memory Analytics |  | **Y** |  |
| Task Management |  | **Y** |  |
| Timelines |  | **N** |  |
| Absences |  | **N** |  |
| Timesheets |  | **N** |  |
| Expenses |  | **Y** |  |
| Requisition requests |  | **Y** |  |
| Approvals |  | **Y** |  |
| Financial Information Centre |  | **Y** |  |
| Budget Books |  | **Y** |  |
| Modeller |  | **Y** |  |
| Planner |  | **Y** |  |
|  |  |  |  |
| **Modules Required (in addition to a selected Engine)** |  | **Required Y/N** | **Notes** |
| Timesheets (not currently in a Product Engine) |  | **N** |  |
| Expenses (included with HR Engine) |  | **Y** |  |
| People Planner (included with Project Engine) |  | **N** |  |
| Position Register (included with Project Engine) |  | **N** |  |
| Salary Review (included with Payroll Engine) |  | **N** |  |
| Cash & Consolidation (not in a Product Engine) |  | **N** | Not required. |
|  |  |  |  |
| **Experience Packs** |  | **Required Y/N** | **Notes** |
| Absence | XPS01 | **N** | Part of HR. |
| Expenses | XTT01 | **Y** | Part of HR. |
| Timesheets | XTF01 | **N** | Not included in a Product Engine. |
| People Planner | XRS10 | **Y** | Part of Projects. |
| Project Planner | XRS20 | **Y** | Part of Projects. |
| Modeller | XCR01 | **Y** | Part of Core Engine. |
| Dates on Relation | DOR | **Y** | Part of Core Engine. |
| Task Management | XT101 | **Y** | Part of Core Engine. |
| Collaborator | XIC01 | **Y** | Part of Core Engine. |
| Timelines | XTL01 | **Y** | Part of Core Engine. |
| Analyser | IAN | **Y** | Part of Core Engine. |
| Financial Information Centre | IIK | **Y** | Part of Accounting / Financials. |
|  |  |  |  |
| **UK Software Engines** |  | **Required Y/N** | **Notes** |
| **UK Localisation Pack - Finance & Procurement** |  |  |  |
| Agresso Standard Report Templates | XRT | **Y** |  |
| Agresso Data Import Utilities suite | IFACE | **Y** |  |
| Agresso Automatic Batch Input | ABI | **Y** |  |
| Agresso Address Interface | ADL | **Y** |  |
| Agresso Bank & Sort Code Validation (This is NOT Albany eVerify. Interface only) | BSCVEL | **Y** | For Bottomline PTX Verify Service which needs to be acquired from Unit4 and already costed in price. |
|  |  |  |  |
| Agresso Receipt Printing | LRE | **Y** |  |
| Agresso Periodic Supplier Payments | SPP | **Y** |  |
| Agresso National Fraud Initiative | NFI | **N** |  |
| Agresso Legal Debt Recovery - Local Government | LDR | **N** |  |
| Agresso Integrated Financials Interface (Student Record interface - Education Only) | FPI | **N** |  |
| Agresso HMRC Message Centre | HMRC | **Y** |  |
| Agresso Construction Industry Scheme | CIS | **N** |  |
| Agresso Construction Industry Scheme with HMRC Message Centre | CISMC | **Y** | Includes HMRC Message Centre and Construction Industry Scheme. |
| Agresso UK Direct Debit bank interface (AUDIS / ADDACS) | DDS | **Y** |  |
| Agresso Bank Statement Auto Import Standard Interface File | BRI | **Y** | Bank import for bank reconciliation. |
| Agresso AP/AR automatic allocation | ARM | **Y** |  |
|  |  |  |  |
| Agresso XML e-Invoicing | XMLEI | **Y** |  |
| Agresso eProcurement - Punch Out | PUNO | **Y** |  |
| Agresso eProcurement - Electronic Purchase Orders | EPO | **Y** |  |
| \* |  |  |  |
| **UK Localisation Pack - HR & Payroll** |  |  |  |
| Agresso Standard Report Templates | XRT | **N** |  |
| Agresso Data Import Utilities suite | IFACE | **N** |  |
| Agresso Automatic Batch Input | ABI | **N** |  |
| Agresso Address Interface | ADL | **N** |  |
|  |  |  |  |
| Agresso Pensions Auto Enrolment | AUNER | **N** |  |
| Agresso HESA Staff Returns (Education Only) | HEASASR | **N** |  |
| Agresso Recruitment Interface | ERI | **N** |  |
| Agresso HMRC Message Centre | HMRC | **N** |  |
| Agresso Bank & Sort Code Validation (This is NOT Albany eVerify. Interface only) | BSCVEL | **N** |  |
| Agresso ABW Local UK Payroll | UKPAY | **N** |  |
|  |  |  |  |
| **Group Pricing - Localisation packs** |  | **Required Y/N** | **Notes** |
| UK localisation | TUK | **Y** |  |
|  |  |  |  |
| **Other Chargeable or Potential Chargeable Items** e.g. Interfaces |  | **Required Y/N** | **Notes** |
| Interfaces |  | **Y** |  |

The following software items are included but no longer listed as separate items:

|  |
| --- |
| Unit 4 Excelerator |
| Unit 4 Data Load and Interfaces Suite |
| Unit 4 Document Archive |
| Unit 4 Identity Services |
| Self Service features:   1. Reporting 2. Expenses 3. Timesheets 4. Tasks 5. Mobile Me |

### Number of User Licences:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Enterprise** | **Professional** | **Business** | **TOTAL** |
| **Number of Users** | **10** | **40** | **1300** | **1350** |