# G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

**G-Cloud 13 Call-Off Contract**

## Part A: Order Form

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier's prepopulated version unless it has been carefully checked against template drafting.

| | |
|---|---|
| **Platform service ID number** | 6603 9270 3644 257 |
| **Call-Off Contract reference** | C162527 |
| **Call-Off Contract title** | Project Portfolio Management (PPM) Software |
| **Call-Off Contract description** | Project Portfolio Management (PPM) application including cloud hosting, support and other associated services. |
| **Start date** | 11/04/2023 |
| **Expiry date** | 10/04/2026 |
| **Call-Off Contract value** | Initial contract value: £113,152 ex. VAT<br><br>Total contract value (including Year 4 and growth up to 225 users): £220,900 ex. VAT |
| **Charging method** | Payment via BACS |
| **Purchase order number** | To be confirmed after contract signature |

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Services offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

| | |
|---|---|
| **From the Buyer** | NHS Business Services Authority<br><br>Stella House<br><br>Goldcrest Way<br><br>Newburn Riverside<br><br>Newcastle-Upon-Tyne<br><br>NE15 8NY |
| **To the Supplier** | TMI Systems Limited,<br><br>Beechey House,<br><br>87 Church Street,<br><br>Crowthorne,<br><br>England,<br><br>RG45 7AW<br><br>Company number 06667738 |
| **Together the 'Parties'** | |

Principal contact details

**For the Buyer:**

REDACTED

**For the Supplier:**

REDACTED

## Call-Off Contract term

| Start date | This Call-Off Contract Starts on **11th April 2023** and is valid for **36 months**. |
|---|---|
| **Ending (termination)** | The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6).

The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1). |
| **Extension period** | This Call-Off Contract can be extended by the Buyer for **one** period of up to 12 months, by giving the Supplier **one month's** written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.

Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance:

https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service |

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:<br>● Lot 2: Cloud software |
| **G-Cloud Services required** | The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:<br><br>● *Verto365* **application licencing;**<br>● **Cloud hosting services;**<br>● **Support services; and**<br>● **Other associated services including but not limited to implementation, configuration, training, data migration, reporting writing, integrations, business process reviews/workshops and offboarding.** |
| **Additional Services** | Not applicable. |
| **Location** | The Services will be delivered to **Stella House, Goldcrest Way, Newburn Riverside, Newcastle-Upon-Tyne, NE15 8NY.** |
| **Quality Standards** | The quality standards required for this Call-Off Contract are **as follows :**<br><br>The quality standards required for this Call-Off Contract are Verto Service as stated within Schedule 1: Services, Appendix B (Service Definition) |

| | |
|---|---|
| **Technical Standards:** | The technical standards required for this Call-Off Contract are Verto Service as stated within Schedule 1: Services, Appendix B (Service Definition) |
| **Service level agreement:** | The service level and availability criteria required for this Call-Off Contract are Verto Service as stated within Schedule 1: Services, Appendix B (Service Definition) |
| **Onboarding** | The onboarding plan for this Call-Off Contract is **as detailed in Performance of the Service of this Order Form.** |

| | |
|---|---|
| **Offboarding** | The offboarding plan for this Call-Off Contract is **as detailed in Performance of the Service of this Order Form**. |
| **Collaboration agreement** | Not applicable. |
| **Limit on Parties' liability** | Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed **£200,000** per year.<br><br>The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed **£200,000** or **125%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).<br><br>The annual total liability of the Supplier for all other Defaults will not exceed the greater of **£200,000** or **125%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). |

| | |
|---|---|
| **Insurance** | The Supplier insurance(s) required will be:<br>● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract<br>● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law)<br>● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law |
| **Buyer's responsibilities** | The Buyer is responsible for provision of device and internet access; data entry, system access, end user support and management.<br><br>The Buyer will provide the Supplier with sufficient information about its project, programme and portfolio management processes for the Supplier to configure Verto for use by the Buyer. |
| **Buyer's equipment** | The Buyer's equipment to be used with this Call-Off Contract includes **users' devices, which must be capable of running a supported browser (vendor-supported versions of Chrome, Edge and Safari)**.<br><br>Reason **is to access to the SaaS application**. |

Supplier's information

| | |
|---|---|
| **Subcontractors or partners** | Microsoft Azure, through Bytes (Microsoft Partner of the Year 2022) |

|  |  |
|---|---|
|  |  |

## Call-Off Contract charges and payment

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

| | |
|---|---|
| **Payment method** | The payment method for this Call-Off Contract is **BACS**. |
| **Payment profile** | The payment profile for this Call-Off Contract is monthly in arrears and is detailed below:<br><br>**Initial Order**<table><tr><th>Charge Ref</th><th>Quantity</th><th>Payment Details</th></tr><tr><td>REDACTED</td><td>REDACTED</td><td>REDACTED</td></tr></table><br>**Orders placed at each Anniversary Date**<table><tr><th>Charge Ref</th><th>Quantity</th><th>Payment Details</th></tr><tr><td>REDACTED</td><td>REDACTED</td><td>REDACTED</td></tr></table><br>**Orders for any additional Services requested throughout the Term**<table><tr><th>Charge Ref</th><th>Unit</th><th>Payment Details</th></tr><tr><td>REDACTED</td><td>REDACTED</td><td>REDACTED</td></tr></table> |
| **Invoice details** | The Supplier will issue electronic invoices in accordance with the Payment Profile detailed in this Order Form. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice. |
| **Who and where to send invoices to** | Invoices will be sent to:<br><br>Email (preferred delivery method): nhsbsa.accountspayable@nhs.net<br><br>Address:<br>NHSBSA Accounts Payable |

| | |
|---|---|
| | Stella House<br>Goldcrest Way<br>Newburn Riverside<br>Newcastle-Upon-Tyne<br>NE15 8NY |
| **Invoice information required** | All invoices must include the following:<br>• each individual Charge as a separate line item;<br>• the Call-Off Contract Reference; and<br>• the applicable Purchase Order Reference. |
| **Invoice frequency** | Invoices will be sent to the Buyer in accordance with the Payment Profile. |
| **Call-Off Contract value** | Initial contract value: £113,152 ex. VAT<br><br>Total contract value (including Year 4 and growth up to 225 users): £220,900 ex. VAT |
| **Call-Off Contract charges** | The breakdown of the Charges is detailed in Schedule 2: Call-Off Contract charges.<br><br>The breakdown of the initial Order is as follows:<br><br>(see table below) |

| Item | Price Per Unit | Quan-tity | Subtotal | One-Off Charges | Annual Charges |
|---|---|---|---|---|---|
| REDACTED | RE-DACTED | RE-DACTED | RE-DACTED | RE-DACTED | RE-DACTED |
| | | | TOTAL | RE-DACTED | RE-DACTED |
| Total for Initial Order (3 Years) | | | | | RE-DACTED |

## Additional Buyer terms

| | |
|---|---|
| **Performance of the Service** | This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones:<br><br>Onboarding<br>The onboarding process is detailed at a high-level in the 'Timelines' section and Paragraph 4.1 of the Service Definition.<br><br>The Parties will jointly develop and baseline a detailed Implementation Plan within 30 calendar days of the Start Date to meet the Buyer's required timescales.  The Implementation Plan will include agreed milestones and the associated acceptance criteria for each milestone.<br><br>Any changes to the baselined Implementation Plan must be mutually agreed in writing between the Supplier and Buyer's project manager.<br><br>In the event that milestones in the Implementation Plan are not Delivered on time due to Supplier cause, the Supplier shall provide a refund of any unused Charges incurred by the Buyer during that delay period.<br><br>Offboarding<br>The exit plan is detailed at a high-level in the Service Definition, Paragraph 4.2.<br><br>An additional exit plan may be required in accordance with Part B: Clause 21 in the event that the Extension Period is activated.<br><br>Contract Management<br>The Supplier will comply its obligations in the Contract Management Requirements and Supplier Response for CMR1.1 to CMR1.5, as detailed in Schedule 1: Services, Appendix B Supplier Clarification Response.  This will be at no additional Charge to the Buyer. |
| **Guarantee** | Not applicable. |
| **Warranties, representations** | Not applicable |
| **Supplemental requirements in addition to the Call-Off terms** | Not applicable. |

| | |
|---|---|
| **Alternative clauses** | These Alternative Clauses, which have been selected from Schedule 4, will apply:<br><br>Not applicable. |
| **Buyer specific amendments to/refinements of the Call-Off Contract terms** | The following definition is added into Schedule 6: Glossary:<br><br>"Anniversary Date" means the anniversary of the Start Date for each Year during the Term. |
| **Personal Data and Data Subjects** | Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: **Annex 1 only** |
| **Intellectual Property** | Intellectual Property Rights are:<br><br>• 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<br>• 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<br>all other rights having equivalent or similar effect in any country or jurisdiction<br><br>Perpetual licences extend beyond the Term and may be terminated solely by the Buyer by providing an express written termination notice. Perpetual licences can be assigned and reassigned by NHSBSA to named internal and external users, as authorised by the Verto Administrator at NHSBSA. |
| **Social Value** | The social value commitments are detailed in Schedule 1: Services, Appendix A (Requirements and Clarification Response), Part B (Social Value Questions).<br><br>In addition to this, the Supplier shall commit to investigating signing onto the Armed Forces Covenant during the Term. |

## 1. Formation of contract

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

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

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

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

## 2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13 .

| **Signed for and on behalf of the Buyer** |
|---|
| REDACTED |

| **Signed for and on behalf of the Supplier** |
|---|
| REDACTED |

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

# Customer Benefits

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

[G-Cloud 13 Customer Benefit Record](#)

# Part B: Terms and conditions

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

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

1.2     This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3     The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

1.4     The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 24 months.

## 2.     Incorporation of terms

2.1     The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)

- 24 (Conflicts of interest and ethical walls)

- 25 (Publicity and branding)

- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

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

2.2.2   a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'

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

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

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

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

## 3.     Supply of services

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

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

## 4.    Supplier staff

4.1    The Supplier Staff must:

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

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

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

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

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

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

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

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

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

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

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

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

## 5.    Due diligence

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

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

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

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

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

## 6. Business continuity and disaster recovery

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

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

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

## 7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 9.    Insurance

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

9.2     The Supplier will ensure that:

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

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

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

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

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

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

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

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

## 10.    Confidentiality

10.1    The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause 34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

## 11.    Intellectual Property Rights

11.1    Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.

11.3    The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:
(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
(b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
(c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

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

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

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

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

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

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

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

11.8 Clause 11.6 will not apply if the IPR Claim is from:

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

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

## 12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

## 13. Buyer data

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

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

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

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

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

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

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

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.cpni.gov.uk/content/adopt-risk-managementapproach and Protection of Sensitive Information and Assets:
https://www.cpni.gov.uk/protection-sensitive-information-and-assets

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: https://www.ncsc.gov.uk/collection/risk-management-collection

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint:
https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance:
https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

13.6.6 Buyer requirements in respect of AI ethical standards.

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

## 14.   Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2    The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

14.3    If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4    If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5    The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

## 15.    Open source

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

15.2    If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

## 16.    Security

16.1    If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2    The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3    If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4    Responsibility for costs will be at the:

16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier,

unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided

16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

## 17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

## 18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover all the Supplier's avoidable costs or Losses

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable

steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4    The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

    18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

    18.4.2 any fraud

18.5     A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

    18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

    18.5.2 an Insolvency Event of the other Party happens

    18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6    If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7    A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.


## 19.    Consequences of suspension, ending and expiry

19.1    If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2    Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the ordered G-Cloud Services until the dates set out in the notice.

19.3    The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4     Ending or expiry of this Call-Off Contract will not affect:

    19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses
- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)

- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

## 20. Notices

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

- Manner of delivery: email

- Deemed time of delivery: 9am on the first Working Day after sending

- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

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

## 21. Exit plan

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

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

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5    Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6    The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

21.6.3 there is no vendor lock-in to the Supplier's Service at exit

21.6.4 it enables the Buyer to meet its obligations under the Technology Code Of Practice

21.7    If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8    The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

## 22.    Handover to replacement supplier

22.1    At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

22.1.2 other information reasonably requested by the Buyer

22.2    On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3    This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

## 23.    Force majeure

23.1    If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other Party may End this Call-Off Contract with immediate effect by written notice.

## 24.    Liability

24.1    Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of two hundred thousand pounds (£200,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2    Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3    Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

## 25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

## 26. Equipment

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

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

## 27. The Contracts (Rights of Third Parties) Act 1999

27.1   Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

## 28. Environmental requirements

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

28.2   The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

## 29. The Employment Regulations (TUPE)

29.1   The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and  (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2   Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

29.2.1      the activities they perform

29.2.2      age

29.2.3      start date

29.2.4      place of work

29.2.5      notice period

29.2.6      redundancy payment entitlement

29.2.7      salary, benefits and pension entitlements

29.2.8      employment status

29.2.9      identity of employer

29.2.10     working arrangements

29.2.11     outstanding liabilities

29.2.12     sickness absence

29.2.13     copies of all relevant employment contracts and related documents

29.2.14     all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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

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

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

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

29.5.1 its failure to comply with the provisions of this clause

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

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

29.7 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

## 30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

## 31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2    In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

## 32.    Variation process

32.1    The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2    The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3    If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this CallOff Contract by giving 30 days notice to the Supplier.

## 33.    Data Protection Legislation (GDPR)

33.1    Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

# Schedule 1: Services

The Supplier will provide the Services required from the Platform Service ID Number specified in the Order Form.  The Services to provided are detailed in Appendix A (Requirements and Clarification Response) and Appendix B (Service Definition) to this Schedule.

Appendix A (Requirements and Clarification Response)

Part A (Statement of Requirements)

# NHS Business Services Authority

## Statement of Requirements

## Project & Programme Management Tool

Project Ref: 1128
Workplan Ref: W15493

# Introduction

The NHS Business Services Authority (NHSBSA) is a Special Health Authority and an Arm's Length Body of the Department of Health and Social Care (DHSC). It provides a range of critical central services to NHS organisations, NHS contractors, patients and the public.

Our services include:

- Processing around 1 billion prescription items for pharmacists who have dispensed prescriptions in England;
- Managing the NHS Pension Scheme in England for over 2.6 million users;
- Administering the European Health Insurance Card (EHIC) scheme in the UK;
- Managing payments to dentists for NHS work in England and Wales – we process 44 million dental forms for payments amounting over £2.5 billion;
- Compiling, publishing and distributing the NHS Drug Tariff for England and Wales;
- Managing NHS Student Bursaries in England, making payments of over £500 million to over 80,000 students;
- Managing the Social Work Bursaries Scheme in England, making payments of over £82 million to nearly 14,000 students; and
- Administering the low income scheme, maternity and medical exemption schemes, tax credit exemption cards and prescription prepayment certificates in England – we process over 5 million claims for these schemes every year.
Further information on the NHSBSA can be found at our website: https://www.nhsbsa.nhs.uk/what-we-do .

# Background

The significant size of the NHSBSA portfolio demands that the project and programme management functions and activity are carried out in a fit for purpose application which supports the appropriate level of governance, assurance, monitoring and decision making by the NHSBSA Leadership Team.

A centralised information repository system allows us to continue working in a more robust and efficient way for managing the NHSBSA portfolio, programmes and projects successfully and timely delivery of business objectives whilst aligning with UK Government Functional standards.

The NHSBSA manages a large portfolio of projects and programmes (circa 50-60 live projects), as part of an overarching enterprise portfolio. The enterprise portfolio is segmented into

several sub-portfolios for each business area who oversee the delivery of their portfolio of projects and initiatives. Whilst this is the most common governance arrangement, it is also possible for major programmes or projects to be governed outside of one of these sub-portfolios and report directly to the enterprise portfolio.

Cora PPM is the system currently used by the NHSBSA. This contract is due to expire in November 2023.

# Scope

- Procurement of a project and programme management application
- 3+1 G-Cloud contract
- Data migration from existing to new application
- Training of all colleagues in the use of the application
- Implementation and integration of the application
- Alignment of the application to NHSBSA Project and Programme Management frameworks
- Alignment of the application to NHSBSA Technology strategy
- Legislative compliance

## Current Users Licence Type

The NHSBSA currently has 145 PPM system users in total. These users vary in terms of the functionality they require, as below:

- 103 full users (all functionality required)
- 22 executive users (directors/senior managers requiring view-only functionality for projects plus the ability to run reports)
- 20 resource users (for submitting timesheets against projects)

## User Growth Estimates

There may be growth in user numbers throughout the contract. The high-level estimate for potential growth is up to a total of 225 users.

## Requirements

**** The word "Gate" was replaced with the word "**** The word "Gate" was replaced with the word "will be assigned a dedicated Client Success Manager, who are on hand throughout the life of the contract, as well as our support helpdesk for administrators." to make the terminology more user friendly for suppliers and NHS agnostic.

Stage" to make the terminology more user friendly for suppliers and NHS agnostic.

**Priority**

*M = Must Have*

*S = Should Have*

*C = Could Have*

| 1. Business Requirements | | | |
|---|---|---|---|
| | **1.1 General Requirements** | | **TMI Response (REDACTED)** |
| **BR 1.1.1** | The supplier must have the ability to deliver training, test and production environments. | | |
| **BR 1.1.2** | The log in screen must allow the NHSBSA to reference the NHSBSA Security Policy and Accessibility statements. | | |
| **BR 1.1.3** | Non-system users (a named resource) must be added within the Solution without the need for a license. | | |
| **BR 1.1.4** | The solution must be fully deployed and live to NHSBSA users by 09/2023. | | |
| | **1.2 Information Governance** | | |
| **BR 1.2.1** | Any solution must be subjected to an IT Health Check in line with the Cabinet Office Guidance by a CREST approved independent organisation. These tests must take place before 'go-live' of the service, after any significant changes to the provided service, and at least on an annual basis. | | |
| **BR 1.2.2** | The solution must be compliant with the requirements and controls of ISO27001. The Statement of Applicability and current certification is | | |

| | | | |
|---|---|---|---|
| | to be provided for validation. | | |
| BR 1.2.3 | UK based businesses must be registered with the Information Commissioners Office. EU based businesses must be registered with their relevant Data Protection Authority. | | |
| BR 1.2.4 | The solution must be GDPR compliant and up to date Privacy notice available to the public on our website. | | |
| BR 1.2.5 | The solution must have automated data retention processes. | | |
| BR 1.2.6 | The supplier must have UK GDPR compliant contracts in place with all sub-contractors. | | |
| BR 1.2.7 | The supplier should be UK GDPR compliant Data Protection and Records Management Policies. | | |
| BR 1.2.8 | Use of personal data must be subject to a Data Protection Impact Assessment DPIA with an appropriate DPIA process is in place, where applicable. | | |
| BR 1.2.9 | The supplier should assist with a Data Protection Impact Assessment, where appropriate. | | |
| BR 1.2.10 | The solution should provide function for staff to view/download all of their own information held within the system. | | |
| BR 1.2.11 | The solution's use of cookies must be in accordance with the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011. | | |
| BR 1.2.12 | The supplier should have and follow documented processes to stay current on emerging vulnerabilities and can demonstrate capabilities | | |

| | | | |
|---|---|---|---|
| | to address new 'zero day' vulnerabilities. https://www.ncsc.gov.uk/ guidance/vulnerability-management | | |
| BR 1.2.13 | The supplier must ensure they have adequate controls in place to perform configuration management, quality assurance and processes to test code quality or vulnerabilities. | | |
| BR 1.2.14 | The supplier must ensure that they assure security through the product life cycle. | | |
| BR 1.2.15 | Data sanitisation and equipment disposal must meet the NHS Digital Guidelines. https://www.ncsc.gov.uk/ guidance/secure-sanitisation-storage-media | | |
| BR 1.2.16 | The supplier must ensure that adequate access controls; both system and physical are in place. This includes (this list is not exhaustive): • The protection and storage of customer data. • Data retention policy. • Destruction of data at contract end. | | |

| 2. Functional Requirements | | | |
|---|---|---|---|
| | **FR 2.1 Project and Programme Management** | | **TMI Response** (REDACTED) |
| FR 2.1.1 | The solution must have the ability to link child projects to parent programmes and child projects and programmes to parent portfolios, or directly to the overall enterprise portfolio. | | |
| FR 2.1.2 | The solution must enable the users to view projects and programmes details, such as risks, issues, assumptions, constraints, financial data, and benefits. | | |

| | | | |
|---|---|---|---|
| **FR 2.1.3** | The solution must enable users to enter and update project information. e.g., project zone, project priority, project status, project stage | | |
| **FR 2.1.4** | The solution must enable users to create and maintain a Project Schedule. | | |
| **FR 2.1.5** | The solution could enable users to map stakeholders. | | |
| **FR 2.1.6** | The solution must enable users to record the state of portfolio, project or programme. e.g., zone level, priority level, stage level | | |
| **FR 2.1.7** | The solution must enable users to record the overall project health, and for key project metrics, such as finances, milestones, dependencies. | | |
| **FR 2.1.8** | The solution must enable users to add stakeholders into projects. | | |
| **FR 2.1.9** | The solution must enable users to add summary statements on the state of a project. E.g., zone level, priority level, stage level | | |
| **FR 2.1.10** | The solution should enable users to add summary statements on the state of a portfolio, sub-portfolio, or a programme, e.g., Priority level, percentage of completion. | | |
| **FR 2.1.11** | The solution must enable user to assign priority attribute to projects. e.g., priority from 1 to 6 | | |
| **FR 2.1.12** | The solution must enable NHSBSA system administrator(s) to customise the design of project space without the need to engage the supplier for development. | | |
| **FR 2.1.13** | The solution must have the ability to archive closed project data. | | |
| | **FR 2.2 Assurance and Checkpoints** | | |
| **FR 2.2.1** | The solution must enable users to approve and manage project/programme phases. | | |
| **FR 2.2.2** | The solution must allow users to add, edit and delete | | |

| | | | |
|---|---|---|---|
| | gateway checkpoint criteria e.g., deliverable sign offs. | | |
| **FR 2.2.3** | The solution should have the ability to create project gateway checkpoints templates for different project sizes and project methodologies. | | |
| **FR 2.2.4** | The solution must allow users to upload email or documents for gateway checkpoint criteria in any format to support the governance process. | | |
| **FR 2.2.5** | The solution must have the ability to add, edit and baseline delivery stage review. | | |
| **FR 2.2.6** | The solution should have the ability to assign actions and/or RAG status against the gateway stage for review. | | |
| | **FR 2.3 Risk & Issue Management** | | |
| **FR 2.3.1** | The solution must enable users to log risks and issues at Project, Programme, Sub-Portfolio and Portfolio levels. | | |
| **FR 2.3.2** | The solution must provide unique references to risks and issues. | | |
| **FR 2.3.3** | The solution must have the ability to add RAG (Red, Red-Amber, Amber, Amber-Green, Green) coloured scoring to identified risks and issues and the scoring of risks after mitigation. | | |
| **FR 2.3.4** | The solution must enable users to document mitigation actions for identified risks. | | |
| **FR 2.3.5** | The solution must enable users to assign risk owners and action owners for each risk. | | |
| **FR 2.3.6** | The solution must provide NHSBSA users with the ability to customise risks and issues field with NHSBSA specific categorisation, e.g., adding categories, root cause, without the need of supplier's intervention. | | |
| **FR 2.3.7** | The solution must have the ability to track review dates against risks and issues e.g., | | |

| | | | |
|---|---|---|---|
| | Created Date, Review Date, Closed Date. | | |
| FR 2.3.8 | The solution must allow escalation of Project risks and issues into associated Programmes or Portfolios. | | |
| FR 2.3.9 | The solution could allow linking project level risks to summarised programme level risks. | | |
| FR 2.3.10 | The solution must enable users to identify overdue risks for review. | | |
| FR 2.3.11 | The solution should have the ability to add updates / notes against a risk or issues. | | |
| FR 2.3.12 | The solution should have the ability to audit trail any changes made to risks and issues based on a customised criterion, e.g., date. | | |
| FR 2.3.13 | The solution could have the ability to notify the owner of overdue risks or issues e.g., via email. | | |
| FR 2.3.14 | The solution must have the ability to link a risk directly to an issue. | | |
| FR 2.3.15 | The solution could have the ability to place costs against a risk. (Red, Red-Amber, Amber, Amber-Green, Green) | | |
| FR 2.3.16 | The solution could have the ability to transfer risks to other projects | | |
| FR 2.3.17 | The solution must have the ability to offer users customisable views for the list of risks and issues including the text view. | | |
| FR 2.3.18 | The solution must be able to calculate the overall risk score using the probability and impact. In accordance with NHSBSA Risk Management Framework (reference attached to the appendices). | | |
| FR 2.3.19 | The solution must allow risks to be scored 3 times (Untreated, Current, Target). | | |
| | **FR 2.4 Benefits Management** | | |

| | | |
|---|---|---|
| **FR 2.4.1** | The solution must allow users to register benefits and benefits management plan for projects, programmes, and portfolios. | |
| **FR 2.4.2** | The solution must provide users with the ability to customise fields for benefit types (e.g., financial, non-financial) and the fields for these benefits tracking plans in accordance with NHSBSA Benefits Management Framework (attached in the appendix). | |
| **FR 2.4.3** | The solution must have ability to log dates against benefits, e.g., closed date, review date, benefits realisation date. | |
| **FR 2.4.4** | The solution must provide users with the ability to score benefits using RAG (Red, Red-Amber, Amber, Amber-Green, Green) feature. | |
| | The solution must provide a transparent audit trail to capture all user activities on benefits. | |
| **FR 2.4.5** | The solution must provide users with the ability to enter a Budget holder against a benefit. | |
| **FR 2.4.6** | The solution should have the ability to attach documentation to individual benefits e.g., evidence. Attachments' format (list is not exhaustive): PDF Excel Jpeg. | |
| **FR 2.4.7** | The solution must provide users with the ability to view a breakdown of a particular financial benefit over a minimum of six years period. | |
| **FR 2.4.8** | The solution must be able to show a breakdown view of benefits (annually and quarterly) over a minimum period of six years. | |
| **FR 2.4.9** | The solution must allow users to view selected past year benefits if needed separately from other past years benefits. | |

| | | | |
|---|---|---|---|
| **FR 2.4.10** | The solution must be able to link benefits data to project data. | | |
| **FR 2.4.11** | The solution must allow for the input, recording and reporting of financial and non-financial disbenefits. | | |
| **FR 2.4.12** | The solution must allow benefits records to be closed (e.g., to reflect removal based on exception reports.) | | |
| **FR 2.4.13** | The solution should be able to calculate the difference between forecasted and actual benefits figures to identify variances so that specific adjustments (to allow optimism bias to be analysed) | | |
| | **FR 2.5 Financial Management** | | |
| **FR 2.5.1** | The solution must enable users to review and update the actual spend and forecast for each cost headings for projects, programmes, and portfolios. | | |
| **FR 2.5.2** | The solution must have the ability to categorise expenditure by different types e.g., capital, externally funded, existing revenue. | | |
| **FR 2.5.3** | The solution must enable users to view a flexible number of years of financials both for future and past years, the number of years must be configurable without the need for supplier intervention. | | |
| **FR 2.5.4** | The solution must have the ability to baseline the approved financials with a defined measure that the project will set. | | |
| **FR 2.5.5** | The solution must provide users with a field to record the named finance lead of a Project, Programme, and Portfolio. | | |
| **FR 2.5.6** | The solution must have the ability to input financial data against several fields e.g., business case approved spend, actual costs, forecasted costs, variance. | | |

| | | | |
|---|---|---|---|
| **FR 2.5.7** | The solution must have the ability to enter resources and their hourly rates and roles. | | |
| **FR 2.5.8** | The solution must have the ability to pull through weekly resource timesheets into financial actuals. | | |
| **FR 2.5.9** | The solution should provide a consolidated view of all expense heads and associated spend at project, programme, and portfolio level. | | |
| **FR 2.5.10** | The solution must enable NHSBSA to configure the financial model to manage portfolio finances without the need to engage the supplier for development e.g., create new budget heads for tracking. | | |
| **FR 2.5.11** | The solution could have the ability to add in cost codes against project budgets. | | |
| **FR 2.5.12** | The solution should have ability to break down all financials by category and financial year. | | |
| **FR 2.5.13** | The solution could provide the project delivery roles and rates that are used to develop business case costings across each project/programme and can be rolled up to sub-portfolio/portfolio level. | | |
| | **FR 2.6. Capacity and Demand** | | |
| **2.6.1 Administration/Management** | | | |
| **FR 2.6.1.1** | The solution must be able to add, edit and delete business directorates, departments and sub departments. | | |
| **FR 2.6.1.2** | The solution must be able to create, edit and delete resources and link them to directorates departments or sub departments. | | |
| **FR 2.6.1.3** | The solution must be able to add, edit and delete a payrate for a resource and show the resource's availability. | | |
| **FR 2.6.1.4** | The solution could enable users to add skills profile for each named resource. | | |

| | | | |
|---|---|---|---|
| **FR 2.6.1.5** | The solution must enable users to add named resources to projects and programmes. | | |
| **FR 2.6.1.6** | The solution could enable users to directly update individual calendars to reflect working patterns and availability for named resources. | | |
| **FR 2.6.1.7** | The solution must enable users to request and approve resources via a defined workflow. | | |
| **FR 2.6.1.8** | The solution must have the ability to hold resource data by financial year (April to March). | | |
| **FR 2.6.1.9** | The solution must have the ability to view all forecasted and actual allocations for a named person team/ department / Role / project/ programme/ defined category. | | |
| **FR 2.6.1.10** | The solution could have the ability to notify a user when work is allocated to them. | | |
| **FR 2.6.1.11** | The solution should have the ability to provide historical resource data in the form of forecasted versus actuals. | | |
| **FR 2.6.1.12** | The solution should have the ability to add an unassigned named role to a project. | | |
| **FR 2.6.1.13** | The solution must have the ability to show resource as forecasted or approved. | | |
| **FR 2.6.1.14** | The solution should have the ability for what-if scenario planning and analysis. | | |
| **FR 2.6.1.15** | The solution must be able to assign resources based on a defined time. | | |
| **FR 2.6.1.16** | The solution must be able to show how much time users are allocated to projects against their availability. | | |
| **2.6.2 Capacity** | | | |
| **FR 2.6.2.1** | The solution must have the ability to show and manage capacity levels at name, role and department level. | | |
| **FR 2.6.2.2** | The solution must have the ability to edit capacity at name, role and department level. | | |

| | | | |
|---|---|---|---|
| **FR 2.6.2.3** | The solution should have the ability to notify resource capacity changes and upcoming resource end dates. | | |
| **FR 2.6.2.4** | The solution should have the ability to add notes to identify when a user does not have 100% capacity for projects/programmes. | | |
| **FR 2.6.2.5** | The solution must have the ability to be able to edit capacity at a monthly timeframe level e.g., Jan, Feb, Mar. | | |
| **FR 2.6.2.6** | The solution must have the ability to input configurable capacity and demand values as wte, days and others as deemed appropriate. | | |
| **2.6.3 Time Recording** | | | |
| **FR 2.6.3.1** | The solution must have the ability for a user to input actual time worked against a project/ Programme / Portfolio or any customisable category e.g., Business As Usual/Continuous Improvement | | |
| **FR 2.6.3.2** | The solution must allow users to only book time against projects/programmes they are allocated to. | | |
| **FR 2.6.3.3** | The solution should have the ability to show a user their historic time recording data. | | |
| **FR 2.6.3.4** | The solution should have the ability to show a user their forecasted work allocation. | | |
| **FR 2.6.3.5** | The solution must allow users to import/export timesheets from/to other systems. | | |
| **2.6.4 Planning** | | | |
| **FR 2.6.4.1** | The solution must allow multiple views of the project plan, e.g., Gantt Chart, Breakdown structures. | | |
| **FR 2.6.4.2** | The solution must have the ability to add and edit milestones and their status. | | |
| **FR 2.6.4.3** | The solution must have the ability to add a progress status against a milestone. | | |

| | | | |
|---|---|---|---|
| **FR 2.6.4.4** | The solution must be able to add a RAG rating against milestones. | | |
| **FR 2.6.4.5** | The solution must be able to add notes against a milestone. | | |
| **FR 2.6.4.6** | The solution must have the ability to add dependencies between projects, programmes, portfolio. | | |
| **FR 2.6.4.7** | The solution must have the ability to add and track project tasks with assigned owners. | | |
| **2.6.5 Approval of Demand Resources** | | | |
| **FR 2.6.5.1** | The solution could have the ability to assign sizing to the demand. | | |
| **FR 2.6.5.2** | The solution must allow users to add one or more roles as a demand. | | |
| **FR 2.6.5.3** | The solution must allow for demand to be requested against a particular role on monthly basis. | | |
| **FR 2.6.5.4** | The solution must have the ability for demand to be editable. Configurable user groups will be able to edit permissions. | M | |
| **FR 2.6.5.5** | The solution should have the ability to capture potential demand with potential dates, resources and financials. | | |
| **FR 2.6.5.6** | The solution should show when resource demand is still awaiting approval. | | |
| **FR 2.6.5.7** | The solution must allow an external named resource to be added as approved against the demand. | | |
| **FR 2.6.5.8** | The solution must allow one or more named resource to be added as approved together with their allocated time to fulfil the required demand. | | |
| **FR 2.6.5.9** | The solution must allow for approval to be added at a monthly timeframe level e.g., Jan, Feb, Mar. | | |
| **FR 2.6.5.10** | The solution must have the ability to input configurable approval values as determined by the customer, e.g., whole time equivalent (wte), days. | | |

| | | | |
|---|---|---|---|
| **FR 2.6.5.11** | The solution must allow users who have been approved against a project/programme/task to complete an appropriate timesheet when assigned. | | |
| **FR 2.6.5.12** | Timesheet must allow users to enter the actual working time and the tasks. | | |
| **2.6.6 Timesheets Management** | | | |
| **FR 2.6.6.1** | The solution should send notifications to users who have not completed a timesheet. | | |
| **FR 2.6.6.2** | The solution should allow defined users to submit timesheets on behalf of other users in cases such as long-term absence etc. | | |
| **FR 2.6.6.3** | The solution should enable project managers to approve submitted timesheets for their projects | | |
| **2.6.7 General Capacity and Demand Requirements** | | | |
| **FR 2.6.7.1** | The solution must allow for an understanding of capacity vs demand vs approval at role, project, programme, portfolio, and any other individual level determined by the customer. | | |
| **FR 2.6.7.2** | The solution must show the approval status of demand request. | | |
| **FR 2.6.7.3** | The solution must show if a particular resource is over or under resourced. | | |
| **FR 2.6.7.4** | The solution must allow users to edit the duration of a project. | | |
| **FR 2.6.7.5** | The solution must have a visual showing all resource demand, resource approval and resource gap at project, programme, and portfolio level. | | |
| **FR2.7. Reporting** | | | |
| **FR 2.7.1** | The solution must provide users with the ability to create customisable reports at Portfolio, Programme and Project levels and any other needed levels. Examples include reporting on risks, | | |

| | | | |
|---|---|---|---|
| | issues, dependencies, benefits, and financials. | | |
| FR 2.7.2 | The solution must have a customisable reporting tool / dashboard across Programme and Project levels and any other needed levels, which can be shared, e.g., progress against any plan, breaking down by stakeholder, adding graphs. | | |
| FR 2.7.3 | The solution must have configurable dashboards showing project/programme/portfolio summary, RAG status, milestones and risks and Issues, benefits, financials as a minimum. | | |
| FR 2.7.4 | The solution must provide users with the ability to report benefits by benefits type and category. | | |
| FR 2.7.5 | The solution must allow benefits to be reported by stakeholder type. | | |
| FR 2.7.6 | The solution must have the ability to report on the demand against resource capacity. | | |
| FR 2.7.7 | The solution must have the ability to produce reports on time, recorded for projects, programmes, portfolios, and defined categories. | | |
| FR 2.7.8 | The solution must have the ability to report on resources for items such as availability, capacity, current utilisation of resources, forecasted and approved resources by Portfolio, Programme and Project or any other needed levels. | | |
| FR 2.7.9 | The solution must have the ability to report on milestones by Portfolio, Programme and Project level. | | |
| FR 2.7.10 | The solution must have the ability to produce configurable templates for users to build project highlight reports. | | |
| FR 2.7.11 | The solution could enable the user to customise Highlight Reports to include | | |

| | | | |
|---|---|---|---|
| | subheadings to clearly differentiate between separate aspects of a project. | | |
| **FR 2.7.12** | The solution must have the ability to export to multiple report formats (PDF, CSV, Excel, images...) | | |
| **FR 2.7.13** | The solution should enable data exports to external applications, e.g., excel to be formatted and consistent in the same way it is sorted in the solution without the need for users to format it. | | |
| **FR 2.7.14** | The solution must have the ability to create reports using the Report Wizard. | | |
| **FR 2.7.15** | The solution must have the ability for Out-of-the-box reports functionality. | | |
| **FR 2.7.16** | The solution must be able to save customised reports so that users can be able to re-run them when required. | | |
| **FR 2.7.17** | The solution should be able to run reports using historic information to show where changes have been made. | | |
| **FR 2.7.18** | The solution must have the ability to report on archived data. | | |
| **FR 2.7.19** | The solution must have the ability to report on Project Checkpoint/ Delivery Stage status e.g., Delivery Stage confidence (RAG) e.g., Red would be proceeding through the next stage at risk. | | |
| **FR 2.7.20** | The solution must have the ability to report on project pipeline management | | |
| **FR 2.7.21** | The solution must have the ability to produce a risk matrix / heat map for projects, programmes and portfolios | | |
| **FR 2.7.22** | The solution must have the facility to report different milestone levels at different forums e.g., Project Board, Programme Review Boards, Portfolio Board | | |
| **FR 2.7.23** | The solution could have the ability to notify project/delivery manager | | |

| | | | |
|---|---|---|---|
| | when a project stage /milestone has been exceeded. | | |
| **FR 2.7.24** | The solution could be able to automatically email reports to selected users at configurable set periods, such as for requesting project status reports. | | |
| **FR 2.7.25** | The solution could allow users to add notes when inputting a time sheet. | | |
| **FR 2.7.26** | The solution could allow user to retrospectively amend errors in previous timesheet entries. | | |
| | **FR 2.8. Overall Solution** | | |
| **FR 2.8.1** | The solution must have intelligent search functionality, e.g., the ability to search by keywords. | | |
| **FR 2.8.2** | The solution must provide the ability for admin users to configure and modify fields without the need for supplier intervention. | | |
| **FR 2.8.3** | The solution must enable users to submit support tickets within the system for any issues that need resolving. | | |
| **FR 2.8.4** | The solution should have the ability to provide automated workflow functionality, e.g., for project stage review, demand and capacity approval. | | |
| **FR 2.8.5** | The solution should keep the user informed that it's responding to the user's action, e.g., showing that the page is loading. | | |
| **FR 2.8.6** | The solution should have the ability to apply customised help/guidance on fields. | | |
| **FR 2.8.7** | The solution must allow the dedicated NHSBSA users to identify inactive accounts. | | |
| **FR 2.8.8** | User accounts could be automatically made inactive after a configurable period of non-use of the solution. | | |
| **FR 2.8.9** | The solution should notify a user after a period of inactivity, providing a time | | |

| | | | |
|---|---|---|---|
| | countdown until the point that the solution will time out. | | |
| FR 2.8.10 | The solution must have the ability to create an audit trail of any project attributes changed such as milestones, RAG status, resource & demand .. etc. | | |
| FR 2.8.11 | The solution could have a Document Repository to allow for sharing of content and processes. | | |
| FR 2.8.12 | The solution should enable users to view full details of text on list views where the field is not large enough to display. | | |
| FR 2.8.13 | The solution must have the ability to import/ integrate GANTT charts via tools such as MS Project. | | |
| FR 2.8.14 | The solution must allow for customisation of the login screen to include NHSBSA branding. | | |
| FR 2.8.15 | The solution must have the ability to customise dashboard views at Programme/Project level. | | |
| FR 2.8.16 | The solution should have auto save with undo capability with the ability for users to turn the auto save functionality on/off. | | |

| | 3. Non-Functional Requirements (NFRs) | | |
|---|---|---|---|
| | **NFR 3.1 Security** | | **TMI Response** (REDACTED) |
| NFR 3.1.1 | Cloud solutions must follow the National Cyber Security Centre (NCSC) Cloud Security Principles. https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles<br><br>The supplier must provide details on how the principles are implemented. | M | |
| NFR 3.1.2 | The solution must be able to comply with NCSC Secure Design Principles. | M | |

| | | | |
|---|---|---|---|
| | https://www.ncsc.gov.uk/collection/cyber-security-design-principles | | |
| NFR 3.1.3 | The solution must provide the ability to implement Multi Factor Authentication (MFA). | M | |
| NFR 3.1.4 | The solution must protect data up to classified as OFFICIAL, including sensitive personal data as per UK Government Cabinet Office Guidelines. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf | M | |
| NFR 3.1.5 | Cloud infrastructure (which includes all hardware, software, networks, and the physical data centres that house it all) must be provided within the UK, European Economic Area (EEA), a country deemed adequate by the European Commission or has agreed adequate protections in place for personal data. | M | |
| NFR 3.1.6 | NHSBSA must be informed of any security breach that may impact the service or authority data as soon as the breach has been identified. | M | |
| NFR 3.1.7 | The solution must provide a transparent audit trail of all relevant user activities including create, update, delete, view which can be reported on and interrogated by the Authority. | M | |
| NFR 3.1.8 | The available logs and audit functionality must be documented and accessible to an end user who has the ability to view audit information. | M | |
| NFR 3.1.9 | The supplier must ensure all sensitive data to be encrypted at transit and rest https://www.ncsc.gov.uk/guidance/tls-external-facing-services | | |
| | **NFR 3.2 Usability** | | |
| NFR 3.2.1 | The solution must be easy for users to navigate and find information with the minimum effort. | | |

| | | | |
|---|---|---|---|
| **NFR 3.2.2** | The solution could provide the ability to have single sign on functionality for users (e.g., Azure AD). | | |
| **NFR 3.3 Access Control** | | | |
| **NFR 3.3.1** | The supplier must ensure that the solution is able to provide NHSBA dedicated users with the ability to configure standard role-based access control, with roles to cover (the list below is not exhaustive):<br>- System Administration user<br>- Users<br>- Unlicenced users | | |
| **NFR 3.4 Accessibility** | | | |
| **NFR 3.4.1** | The solution must work with assistive technologies in compliance with compliance with Central Digital and Data Office (CDDO), formerly known as Government Digital Service standards.<br> https://www.gov.uk/service-manual/technology/testing-with-assistive-technologies | | |
| **NFR 3.4.2** | The solution must store and process monetary values as Great British Pounds (GBP), prefix displayed amounts with the pound sign ("£") and to an accuracy of two decimal places (".00"). | | |
| **NFR 3.4.3** | The solution must work across all modern browsers including Google Chrome, Microsoft Edge, Firefox and Safari. | | |
| **NFR 3.4.4** | The solution must be device agnostic i.e. work across all standard device types including pc/laptop (running Windows 10, Linux or MacOSX), mobile or tablet. | | |
| **NFR 3.4.5** | The solution must be AA accessibility compliant as defined by the W3C Web Content Accessibility Guidelines (WCAG) 2.1 | | |
| **NFR 3.4.6** | The solution must be responsive in design to work across different devices and screen resolutions. | | |
| **NFR 3.4.7** | The solution must be able to support at least 150 concurrent users. | | |

| | | **NFR 3.5 Recovery, Reliability & Availability** | | |
|---|---|---|---|---|
| **NFR 3.5.1** | | The supplier must ensure that all planned outages are agreed in advance by all parties. | | |
| **NFR 3.5.2** | | The solution must have an uptime of 99% or higher. | | |
| **NFR 3.5.3** | | The solution must have a Mean Time To Recovery (Information Unavailable) of 12 Hours.<br><br>This is the average time it takes to recover from a system failure where some information is unavailable but not all of the system is affected. | | |
| **NFR 3.5.4** | | The solution should have a Recovery Point Objective (RPO) / Restore time of 24 hours.<br><br>The RPO described the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold. | | |
| **NFR 3.5.5** | | The solution should have a Recovery Time Objective (RTO) / Backup time of 48 hours.<br><br>The RTO is the duration of time and a service level which the application must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity. | | |
| **NFR 3.5.6** | | The solution must have a Mean Time To Recovery (System Down) of 12 hours.<br><br>This is the average time it takes to recover from a system failure where the entire system is down. | | |
| | | **NFR 3.6 Maintainability** | | |
| **NFR 3.6.1** | | The supplier must ensure that an upgrade schedule is agreed in advance by all parties. | | |
| | | **NFR 3.7 Supportability** | | |
| **NFR 3.7.1** | | The solution must be supported Mon-Fri 07:00- 19:00 excluding Bank Holidays. | | |

| | | | |
|---|---|---|---|
| **NFR 3.7.2** | The solution must be supported Mon-Fri 09:00- 17:00 excluding Bank Holidays. | | |
| **NFR 3.7.3** | The supplier must prioritise all support calls in line with NHSBSA SIAM guidelines, e.g. prioritising the support requests in line with NHSBSA prioritisation levels. | | |
| | **NFR 3.8 Performance** | | |
| **NFR 3.8.1** | The supplier must ensure the application is responsive and works in a timely manner in line with industry standards for SaaS products. | | |
| **NFR 3.8.2** | Access to the system must be available 24/7. Normal operating hours are Mon - Fri 7:00 - 19:00, but users must be able to access the system at any time. | | |
| | **NFR 3.9 Interoperability** | | |
| **NFR 3.9.1** | The solution could have the ability to integrate with MS Outlook for email and calendars and MS 365. | | |
| **NFR 3.9.2** | The solution must be able to export in various formats to support further processing e.g. PDF/XLSX/DOCX etc | | |
| | **NFR 3.10 Data Migration** | | |
| **NFR 3.10.1** | The solution must have ability to import data from the existing system as part of a migration. Current Database size is 15GB, with average of 10% growth per year. | | |
| | **NFR 3.11 Database capacity** | | |
| **NFR 3.11.1** | The solution must be able to retain data for a configurable period of time. | | |
| **NFR 3.11.2** | The solution must store the data according to in accordance with NHSBSA Retention Policy | | |
| **NFR 3.11.3** | To solution should allow data to be purged after a period in accordance with NHSBSA Retention Policy | | |
| **NFR 3.11.4** | The solution must be able to scale storage and compute accordingly for existing and future data. | | |
| | **NFR 3.12 Database Performance** | | |

| | | | |
|---|---|---|---|
| **NFR 3.12.1** | The supplier must sure the user interface allows data to be accessed daily with minimal impact on users from any database specific routines such as housekeeping and backups. | | |

| | **Contract Management Requirements** | | **TMI Response** (REDACTED) |
|---|---|---|---|
| **CMR 1.1** | The Supplier should provide a single dedicated point of contact for management of the contract. This person should also be able to delegate this role as required. | S | |
| **CMR 1.2** | Risks and issues relating to the contract should be proactively monitored and reported by the Supplier, with both Parties being responsible for management of their own allocated risks. | S | |
| **CMR 1.3** | The Supplier should monitor and report on their performance against the service levels (i.e. system availability, incident resolution times etc.). | S | |
| **CMR 1.4** | The Supplier should attend monthly operational review meetings (virtual or physical as mutually agreed). These meetings will cover any operational matters and changes to licence numbers throughout the month. | S | |
| **CMR 1.5** | The Supplier should attend quarterly performance review meetings (virtual or physical as mutually agreed). The agenda will be mutually agreed in advance, but is expected to cover: service level performance; risks/issues; updates of licence numbers; updates of contract spend; strategic updates; escalations; and any other business as required. The Supplier is responsible for producing the minutes to formally record all key points, decisions and actions. | S | |

Part B (Social Value Questions)

**atamis ✸ Supplier Portal**

eSourcing Response Document

*3 March 2023*

| | |
|---|---|
| Project Ref and Name: | **C132291 - W15493 [Proc] Project Portfolio Management (PPM) Software** |
| Section: | **3. Social Value (Fighting Climate Change) Envelope** |
| Supplier Name: | **TMI SYSTEMS LTD** |

Social Value

## Carbon Emissions

Detail how, through the delivery of the contract you will commit to undertake and monitor the following: • To provide forecasted baseline for the emissions generated in contract year 1 • What activities you will undertake to reduce emissions generated in the performance of the contract (represented as both tCO2e and as a % of the baseline emissions) • Annual carbon reporting for activities related to the contract. You may include images or diagrams if this supports your answer. Max. word count: 750 (please note that this does not need to be 750 words. It is a maximum allowable word count if suppliers wish to provide that volume of detail). Further clarification could be provided during the demonstration and Q&A session.

*Type:*          Required

REDACTED

## Circular Economy

Please describe how you will support NHSBSA with the following: Business rule 2: Circular economy – resources and waste strategy 2020: All suppliers have circular ICT policies and strategies and products are routinely designed for durability, ease of maintenance and re-cycling. Problematic materials and substances have, or are being, phased out of use. 2025: HMG suppliers have established zero waste to landfill or zero-waste targets. Suppliers are meeting targets to incorporate more recycled materials in their products and eliminate the use of single use plastics. There's a yearly increase in ICT kit purchased/leased that is remanufactured/refurbished. Please note there is no suggested or maximum word count for this. You may include images or diagrams if you wish to support your answer. Further clarification could be provided during the demonstration and Q&A session.

*Type:*          Required

REDACTED

Social Value

# Environmental Management System

The supplier should have processes in place that are compliant with the controls of ISO14001 (this does not necessarily mean the supplier must hold a formal accreditation). Please detail how you support this. If your solution involves a third-party hosting service, please include this detail also where possible.

Please note there is no suggested or maximum word count for this. You may include images or diagrams if you wish to support your answer. Further clarification could be provided during the demonstration and Q&A session.

*Type:* Required

REDACTED

# Influencing Stakeholders

At NHSBSA we view protecting the environment as a priority, for instance when any business travel is considered. Detail how, through the delivery of the contract you will engage and monitor staff, suppliers, customers, and communities in supporting environmental protection and improvement. You may include images or diagrams if this supports your answer. Max. word count: 750 (please note that this does not need to be 750 words. It is a maximum allowable word count if suppliers wish to provide that volume of detail). Further clarification could be provided during the demonstration and Q&A session.

*Type:* Required

REDACTED.

# Net Zero

Please describe how you will support NHSBSA with the following: Business rule 1: To meet net zero by 2035 (or sooner) 2020: All ICT suppliers commit to science-based net zero targets in line with the Paris Agreement (or procuring department target, whichever is sooner) and have developed carbon mitigation and adaptation strategies. 2025: All ICT suppliers follow up the commitment they made to becoming net zero with a road map and action plan, showing proven progress towards the goals. Seeking a carbon positive/net gain/net positive outcome through the services provided. Please note there is no suggested or maximum word count for this. You may include images or diagrams if you wish to support your answer. Further clarification could be provided during the demonstration and Q&A session.

*Type:*      Required

REDACTED

Appendix B (Service Definition)



Work Collaboration platform for everyone

Verto Service Definition

G-Cloud 13

**Verto 365 – functional overview**

Verto 365 is a cloud-based solution that provides a work collaboration platform for the entire organisation.  It manages everything from simple day to day tasks through to major initiatives right across the organisation. It is entirely user configurable supporting multiple workflows and business processes and provides a central repository and single version of the truth for all project and work management requirements.

Key features include:

- Cloud based, accessible everywhere
- MS Teams and O365 integration
- Fully configurable dashboards
- Instant chat messaging
- Alerts and notifications
- Document management and sharing
- Fully configurable project and programme management functionality
- Kanban Board Functionality
- Compatible with finance and HR systems
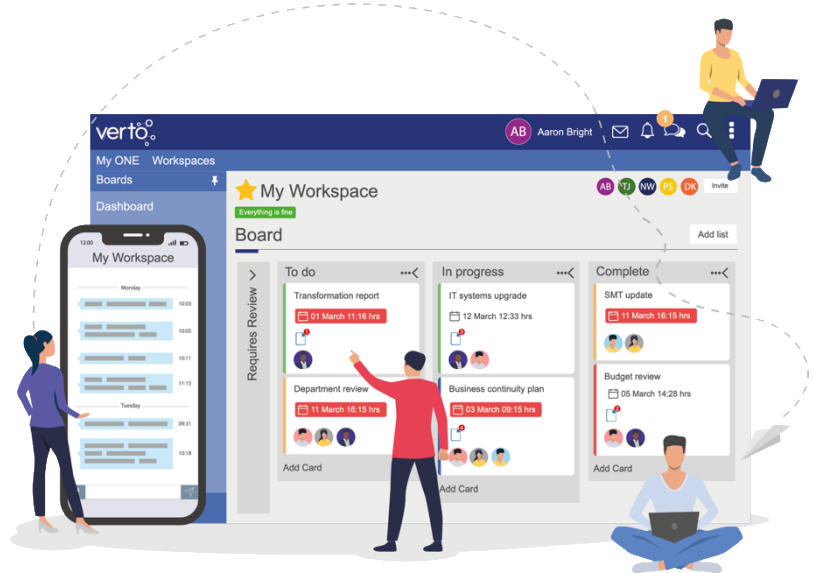


**Kanban Boards**

The Kanban board functionality within Verto 365 allows you to create as many personal or shared boards as you like. Create lists to contain cards of activities at similar stages of completion, for example, and move them around as the activity progresses. Cards can hold information such as statuses, due dates, members, custom tags, additional documents and much more. A variety of templates can help you get started, but you can create your own templates as required.

Every board can be filtered for help finding specific data. For example, you can easily filter a board to only show cards you are a member of, or with a status of red, that is also due in the next 7 days etc. As well as this, all board data can be aggregated and summarised within our dynamic dashboard, providing even more opportunities to filter and group cards across multiple boards at once.
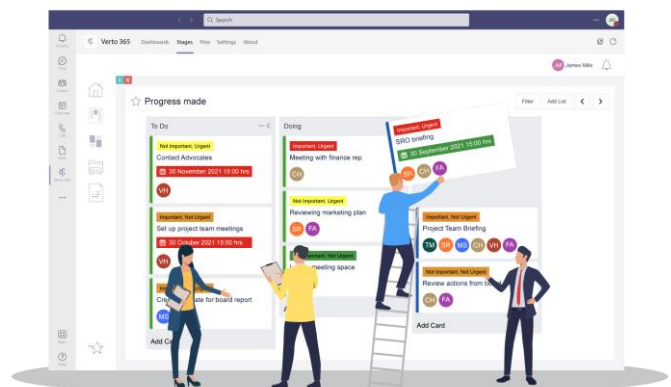


**Dashboard Monitoring**

The Verto 365 dashboard provides a real-time, aggregated view of all project & programme information, focusing on what means most to you, be it milestones, risks, costs or anything you're recording in the system. You can create and save as many dashboards as you wish and share

them with colleagues whenever necessary. The dashboard is interactive at every level and can be fully customised using extensive options of widgets, which can be tailored into several formats (bar charts, line graphs, containers, data tables etc.) to suit your preferences. Each widget can be filtered using any relevant field, providing full control over the management information you would like to focus on at any time.
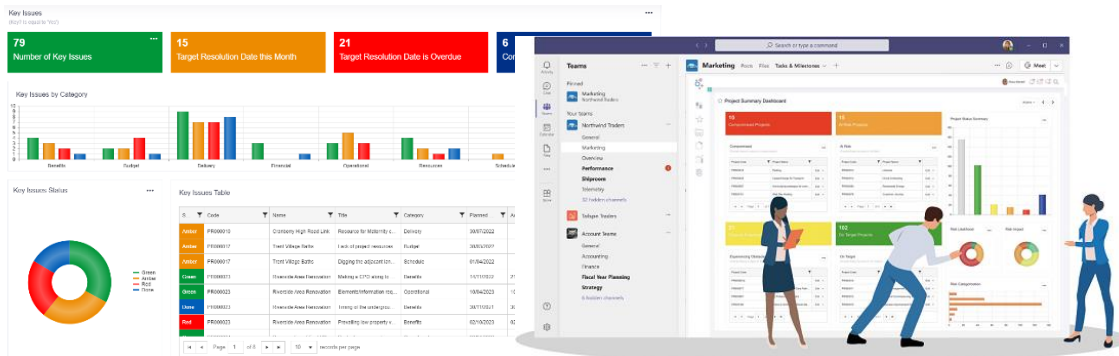


### Reporting

Verto 365 boasts powerful reporting functionalities at multiple levels that allow for reports to be produced based on any and all information within the system. All reports can be exported in a number of different formats including Word, Excel, PDF, CSV, TIFF etc.  All our reports are run in real-time, ensuring that only the latest information is presented.
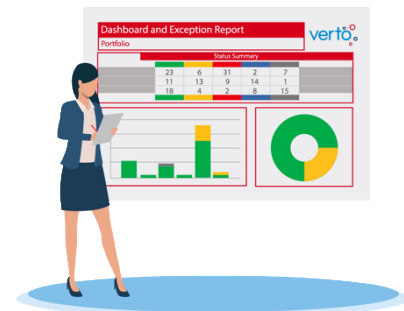


Users can take advantage of our subscription service so that real-time reports received by users in their inbox, eliminating the need to access the system to run a report. We use 'tags and filters' to 'slice and dice' the data as much as required, to further enhance reporting capabilities.

We also produce specific data extracts for reporting tools such as PowerBI, Tableau and QlikView.

### Workflow configuration

Verto 365 has fully configurable workflow that allows workspaces and projects to move through a defined set of stages and approvals. The workflows can be set up in multiple ways by different teams and departments across the organisation according to project size and complexity. They can be customised to incorporate PMO or SMT sign off at any stage. All changes, requests and approvals are recorded providing a complete audit trail.

**Risk Management**

Verto 365 provides comprehensive, configurable Risk and Issue Management functionality that can be held against both the Programme, Project or Workspace and aggregated up to Programme and Portfolio level. Owners can be assigned to individual risks and issues, along with proximity dates and mitigating actions (amongst many other field options). The fields contained both within these functions and others throughout the system can be configured so they perfectly match the registers currently used by the organisation and support governance.

RAID logs can easily be produced and reported at multiple levels, including workstream, project, programme and portfolio.

**Planning / Gantt**

Project plans and schedules can be created simply and managed easily within the system using Verto 365's planning feature. Multiple views are available for users to customise how they view and update plans.

Verto 365 has a Gantt feature embedded within the planning module that provides a visual assessment of project plans. The Gantt view is interactive, allowing for all elements of the planning module to be amended in this format. An 'offset dates' feature is available when an entire plan needs to be pushed back or brought forward as required. Users can import MS Project Plans into Verto 365 allowing them to use their preferred tool whilst supporting team collaboration.

**Dependency Management**

Verto 365 has a feature called 'VertoSense' which allows for dependencies to be identified against any two objects in the system.

This allows for comprehensive dependency networks to be produced from those connections made. For example, connections can be made between a project risk and a project milestone, to identify the dependency that risk may have on the associated milestone.
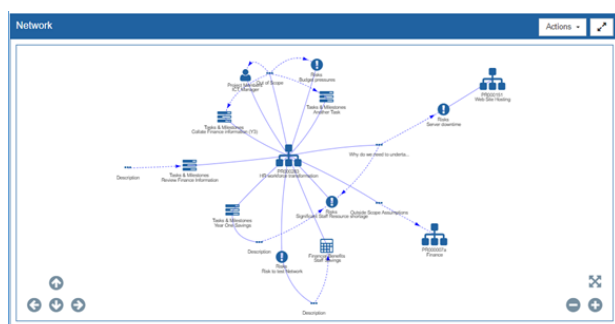
These dependencies can be selected within the system, which then brings up the fields linked with that dependency.
These fields can be amended and updated without having to enter that section, if the user has the correct permissions.

**Benefit Realisation and Cost Management**

Verto 365 records quantitative and qualitative benefits which are then tracked and reported against at multiple levels, via the dashboard as well as utilising our comprehensive reporting functions.

Verto 365 provides full finance management capabilities, allowing users to track cost profiles over time, providing full transparency on project spend. Financial integrations with systems such as SAP, Oracle, Pegasus, Agresso, can be achieved to ensure Verto 365 remains the central repository for analysis / reporting purposes.
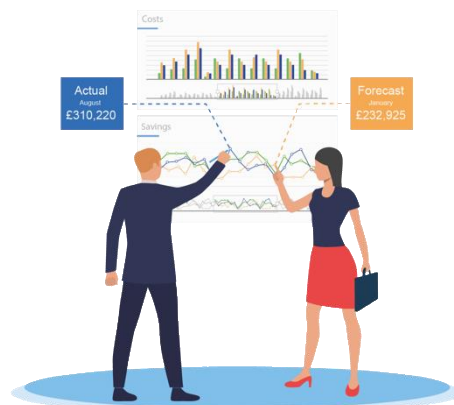
**Audit Trail**

Verto 365 has a comprehensive audit log that is automated against every field in the system. Every change is recorded and is easily viewable by the users.

Changes to fields are also supported by a 'track changes' feature so you can more easily see what's changed between versions.
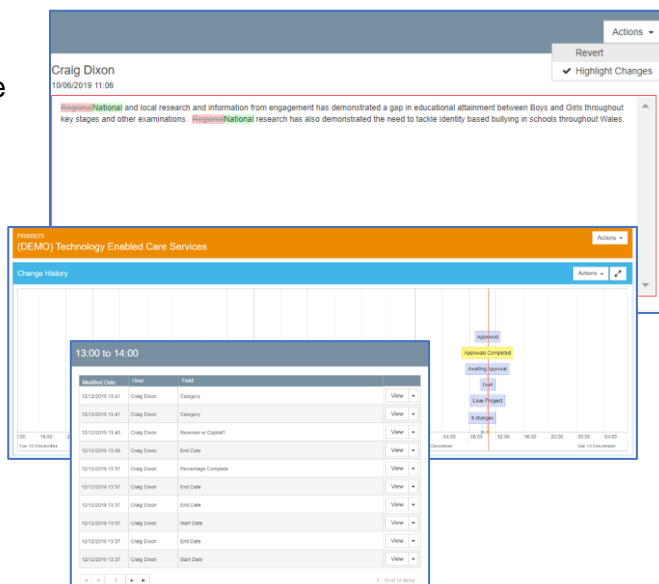
**Storage**

Unlimited, cloud-based storage is available for each entity (e.g. project, programme, portfolio) to manage documents and each document store is independently secured, so that only users with the appropriate permissions have access to it. External links such as a SharePoint archive can be inserted, however Verto 365 also integrates directly with SharePoint, so you can continue using the current storage solution you are familiar with.

**Custom Notifications**

Verto 365 can provide user-defined automated risk alerts and notifications that appropriate to the level of involvement, including approvals, missed dates and other tasks and milestones.

Users can be notified of any changes or updates to any field within the system, including risks. This applies to every field within a risk so nominated users are always notified immediately relevant changes are made by others. Common notifications are, but aren't limited to, a change to the 'proximity date' or 'current risk rating' of a risk.

**Resource Management**

Verto 365 contains comprehensive resourcing functionality which has been designed to ensure you can find the right people for your projects based on availability, skill set and any other information you want to use.

Verto 365 gives you the ability to search across all your resources to see who's available, who's been allocated to which project(s) and when they may be overallocated.

You can search on any criteria you need, be it job title, team, project role, location, specific skill etc., Verto 365 supports your own views/groupings of the resource pool. You can plan as far ahead into the future as you need so you can avoid clashes.
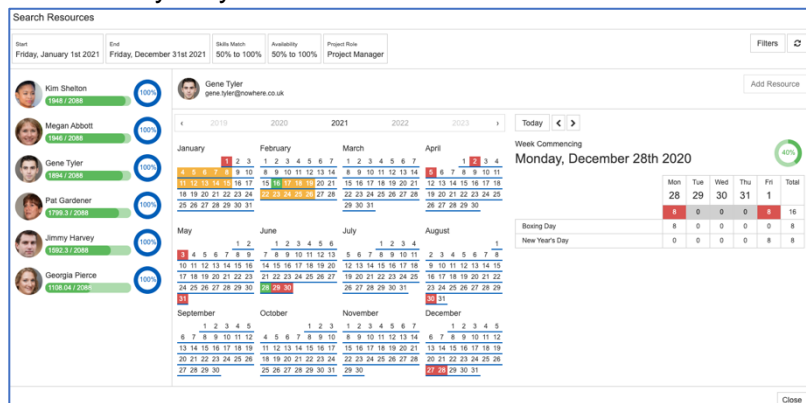


The main resourcing page gives you an 'at a glance' view of a person's allocations across an entire year, making it easy to identify issues and resolve them ahead of time.
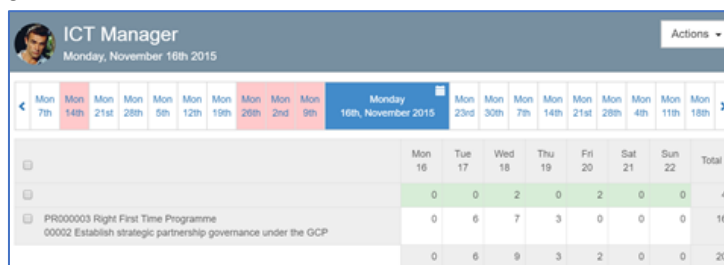
If needed you can then review each person individually to ensure you have the right person for the job.

Individual rates are then calculated so you can get a true picture of the cost of your project. Used in conjunction with the timesheets module you'll be able to see the expected and actual costs of all the time spent.

**Timesheet Management**

Users can complete timesheets within Verto 365 to reflect the actual time spent on completing a task and there is logic built in to make this as quick as possible for the end user. The system knows which projects an individual user is assigned to and will only show the relevant tasks to ensure quick but accurate time recording.

The submissions will then go through an approval before the time is added to the project record.
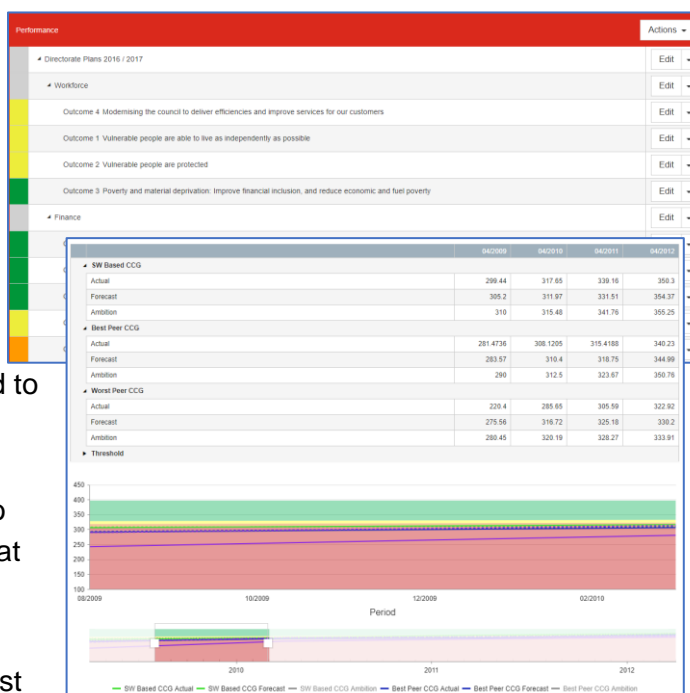


**Performance Management**

The Verto 365 performance management module can be utilised to measure project performance and be reported against using our reporting feature. Pre-set thresholds can be assigned to a KPI that can then be used to measure performance of projects against a particular KPI. Both projects and non-project activities can be assigned to a KPI, to further support performance analysis against projects. Performance groups/objectives can easily be created to ease the management of multiple KPIs that form part of the same objective.



The ability to compare performance against other organisations or services is also available, so you can track your progress against others.

We have a performance management report that is part of our standard suite of reports, however custom reports / plans / graphs can be produced and tailored to suit each organisation's needs. Within the system, a quartile graph is included for each KPI however custom charts / graphs can be produced if required.

**Security / Access**

Administrators have full controls to tailor each users access and involvements within the system. Roles can be assigned to users, to ensure they have access to the correct system elements.

Restrictions can be placed throughout the system, so users will only ever see what is relevant to them. For example, administrators can choose to restrict a user's access from a particular stage, or even to the reports section of the system if required. Verto can be accessed using browsers on mobile devices.

**Credentials**

Our preferred method of authenticating credentials is using Single Sign On where we delegate the authentication process to the customers active directory. Where this is not possible users can provide username/password with 2 factor authentication.

**Integrations**

Verto can be integrated with any accessible system. Our integrations are typically tailored to suit the competing requirements of each client. We have integrated with numerous financial systems (SAP, Agresso, Oracle) as well as numerous identity providers (including active directory) and timesheet management systems.

Verto 365 can be fully embedded within Microsoft Teams. This allows users to manage projects, end to end, within MS Teams without the need to leave their Office 365 suite of tools or log into another system.  The synchronised calendar allows for items such as project tasks, milestones, risks, and issues to be overlayed within the same diary of events and meetings in your MS Teams calendar view. Synchronised document storage allows you to continue managing your documents within SharePoint via Verto 365 and MS teams.

Multiple Kanban boards and dashboards can be added to each project directly within MS Teams, extending collaboration opportunities and providing management information at the user's fingertips.
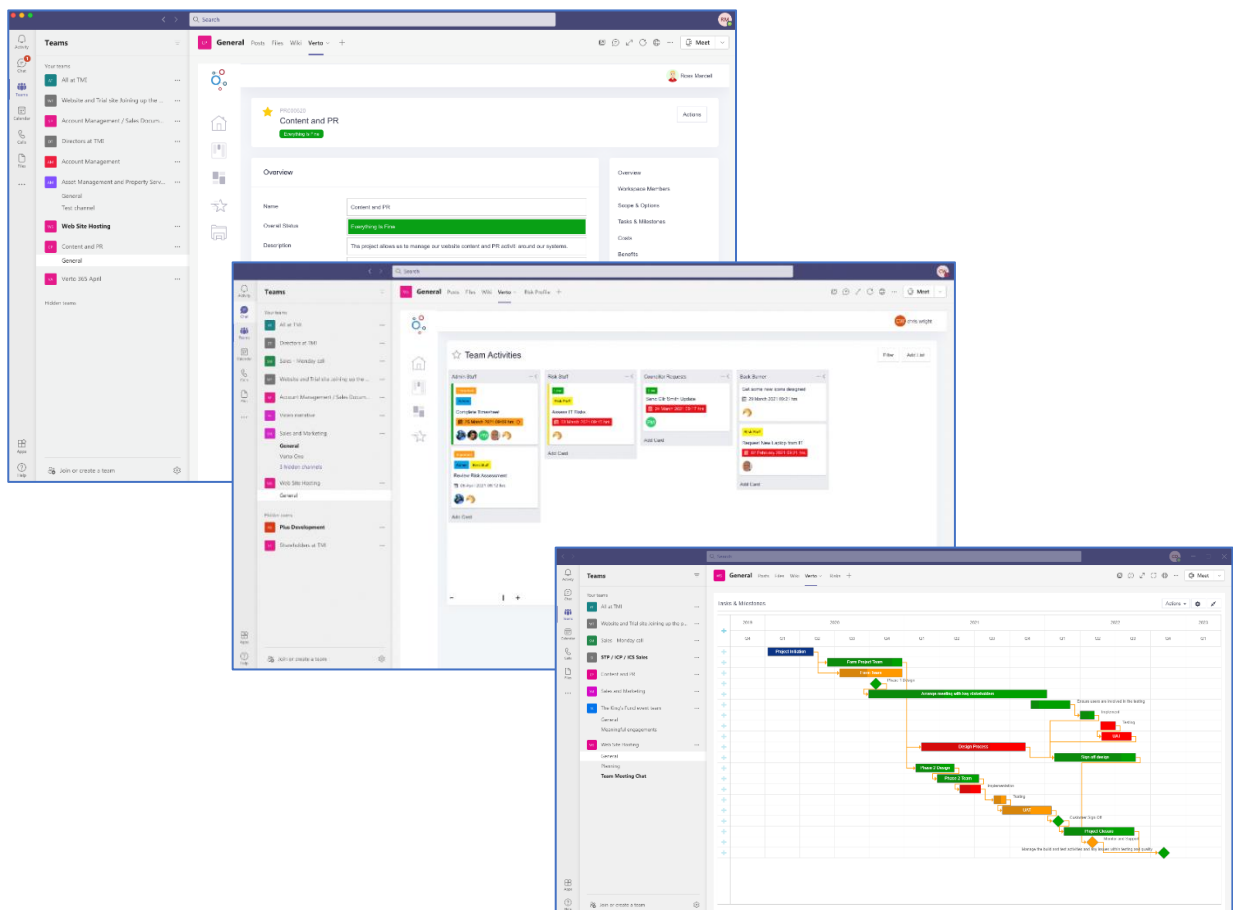
**External Forms**

External forms are used to gather data into Verto 365 that is initially generated outside of the system. Examples would be project idea forms, funding applications and company engagement forms. These submissions can be completed by anyone, they don't need to be a Verto 365 licence holder, so the possibilities are wide-ranging.

Those who complete these external forms will receive an email upon starting a form with a link to give them direct access to pick up where they left off, so they don't have to complete the form in a single sitting. These forms would be configured by your administrators using the same 6,000 plus fields available when configuring stages within Verto 365, this means they'll always perfectly suit your requirements.

All the data submitted will be added directly to the Verto 365 database which means there's no need for re-keying anything, no duplication of effort. It's all reportable and can progress through the normal project stages if needs be.



**Cost and licencing model**

Verto 365 is an entirely cloud-based work collaboration platform available via user licences. User licences are available either on a perpetual licence purchase or an annual licence basis. The licence purchase option provides the lowest cost of ownership for organisations using the service after 2 years. All user licences can be assigned and reassigned to individuals both inside and outside of the organisation as often as required.

As organisations increase their user base the cost of user licences previously purchased or rented are deducted from the cost of new licences.

**Timelines**

Verto 365 is a cloud-based SaaS system meaning there is no need for anything to be installed at the client site. The client organisation will have access to two Verto 365 sites (Test and Live), both of which will be accessible from any device with an internet connection. Whilst new sites are provided 'ready to use' and can be tailored to suit the needs of the client organisation. Working closely with new clients, the development of a comprehensive timeline will be delivered.

Whilst new sites are provided 'ready to use' and can be tailored to suit the needs of the client organisation. Working closely with new clients, the development of a comprehensive timeline will be delivered.

A typical Verto implementation is made up 4 key phases:

| Phase | Summary |
| --- | --- |
| Start Up | During this phase we will work with the client organisation to agree timelines, understand processes and critical success factors. A comprehensive training packages is also delivered in this phase. |
| System Build | During this phase the client organisation will be supported to configure Verto to meet specific requirements. End user acceptance testing and data migration is also delivered in this phase. |
| Go live | During this phase the reconfigured site will be copied to the Live site, ready for the client organisation to rollout. End user training is also delivered in this phase. |
| Post Implementation | During this phase we will work with the client organisation to review the critical success factors and discuss any future needs. Provision of support and consultancy is available help embed and grow Verto across the client organisation. Review meetings will continue to ensure that Verto continues to meet client organisation needs. |

**The Verto System**

The Verto Hosted platform is run in the Amazon Web Services (AWS) environment. ALL data is hosted and processed in their London datacentre. AWS hold ISO9001 and ISO 270001 certifications. Full details of the hosting provider can be supplied on request. Limited API access is available for the uploading of financial (invoice) records from corporate finance systems.

Verto is an entirely Microsoft Windows based platform. An architecture diagram can be supplied on request.

**2.Information Assurance**

Verto data is housed in a UK Tier 3+ datacentre. All data is encrypted in transit using a minimum of TLS1.2 over an HTTPS connection, the nature of the data held is almost universally OFFICIAL and below. No personally identifiable data is held within the database.

3. **Backup / Restore and Disaster Recovery**

      Details of the backup/restore processes can be found in Appendix C - Verto Technical Platform.

      TMI Systems have a disaster recovery plan that is available on request.

4.     On-boarding and Off-boarding processes/scope etc.

## 4.1. On-boarding Process

      The On-boarding Process follows the Verto Implementation Process, which consists of the following steps:
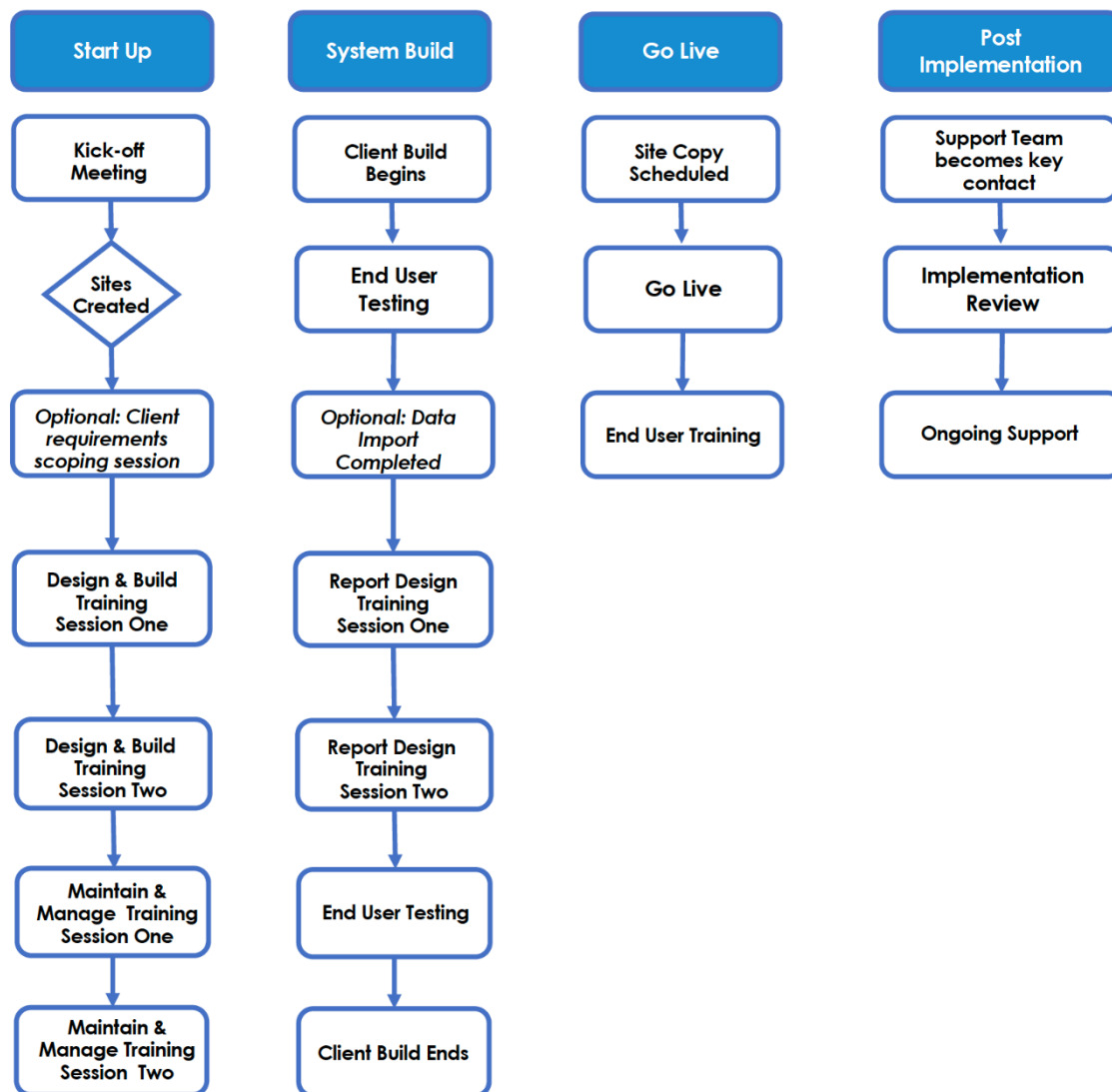


## 4.2. Off-boarding Process

      At the end of any agreement with a Customer, TMI Systems would return all data to the Customer in the form of a SQL Server 2019 (or whatever the currently implemented version of SQL Server is) backup files (Live and Test). These databases would then be deleted from our production systems.

Backups of the Customer's databases would be stopped on the date of termination; however, our backup retention policy of 3 months means that the Customer's data would not be fully eradicated from our backup servers until 3 months had elapsed. This backup will be compressed and made available on our sftp servers for download within 48 hours of contract termination.

We would suggest a provision is made for at least 1-2 service days to cover the following activities:

1. Raise change requests to remove instance
2. Remove Test and Live sites, including configurations from Production Servers
3. Take final backup of Live database.
4. Take final backup of audit database.
5. Remove Test database from production servers
6. Remove Production database from production servers
7. Remove Production mirror form reporting database servers
8. Remove Reporting configuration and reports
9. Remove databases from backup schedules
10. Remove nearline backup schedule
11. Compress and copy production backup to SFTP server
12. Create SFTP user for client (limit access to single folder contain gin backup)
13. Inform Client of SFTP username/password
14. Once download has completed remove backup and store in archive area for 30 days
15. 30 days later – remove archive backup

5. Pricing

# 5.1. Unit based pricing model

Verto is a hosted service (SaaS). Please see our price list for further information.

# 5.2. Aggregated billing options

The user level price model is flexible allowing organisations to use the service as required for example, in specific departments or with partner agencies.

# 5.3. Minimum Contract/Billing Period

The minimum contract period is a 1 year.

# 5.4. Free option

A free service is available. Please see our price list for further information.

# 5.5. Trial Option

A pilot option is available to clients who wish to evaluate the service for up to 20 users for 30 days.

# 5.6. Termination costs

There are no termination costs for Verto

## 5.7.      Supplier contract terms jurisdiction

Our standard terms and conditions are enclosed together with a service level agreement. The system can be accessed by any nominated user on behalf of the purchasing organisation within the UK. (Appendix A – TMI Systems Contract and Appendix B – TMI Systems SLA)

## 5.8.      Payment Options

Our standard payment terms are 30 days from invoice.

6.  Service management details

## 6.1.      Technical boundaries/interfaces of the service.

All technical interfaces are fully documented and available on request.

## 6.2.      Services available to other suppliers.

No services are available to other suppliers.

## 6.3.      On-boarding process.

Please see section 4.1.

## 6.4.      Off-boarding process.

Please see section 4.2.

## 6.5.      Data extraction/removal criteria.

TMI will provide a copy of a customer's database within 24 hours on request. TMI will remove any data from the customer database upon receipt of an official request to do so. Please see section 4.2 (off-boarding) for details on removal of data at the end of contract.

## 6.6.      Data processing and storage locations.

All customer data is stored and processed in the AWS Datacentre in London, UK and is encrypted both in transit and at rest.

## 6.7.      Data location option can be defined by user.

There is no option for the data location to be defined by the user – All data is held in a UK datacentre, see 6.6, 6.9 & 6.10

## 6.8.      Data held in Safe Harbour.

Not Applicable

## 6.9.      Data centre(s) used adhere to best practices described by the EU Code of Conduct for Data Centre Operations

The Data Centre is designed and built to meet rigorous compliance standards across all of the territories in which it operates including the EU Conduct for Data Centre Operations. Further details on their compliance status can be found here:  https://aws.amazon.com/compliance/?nc=sn&loc=3

## 6.10.    Data centre tier.

All hosting services are provided by AWS. Their Data Centres align themselves to Tier 3+ but are closer to Tier 4.

## 6.11.    Support boundaries/interfaces of the service.

Support is via a dedicated helpdesk; details can be found in Section 8.

## 6.12.    Service roadmap.

The roadmap for the service can be provided on request and is updated on a quarterly basis.

## 6.13.    Performance attributes.

Please see Section 8.

## 6.14.    Backup & Disaster Recovery.

Please see Section 3.

## 6.15.    Support service provided.

Please see Section 8.

## 6.16.    'Real time' management information.

Verto provides real-time reporting across all data held within the database.

## 6.17.    Reports include each billed unit.

Reports are tailored to the requirements of the end user and so may or may not include each billed unit, depending on user requirements.

## 6.18.    Self service provisioning/de-provisioning.

Administration users can modify the way in which data is presented to users and so can provision new functions within the application. TMI must be used to provision new instances of the application or new stages. See section 7.2 for further details on user customisations.

## 6.19.    Indicative time for provisioning/de-provisioning.

24 hours.

## 6.20.    3rd party service monitoring tool access.

Many of our customers point their monitoring tools at the Verto landing page since it is cloud based. This allows them to verify that the service is up.

## 6.21. Service Desk can be used by 3rd party suppliers for their services.

No Service Desk provision is available for 3<sup>rd</sup> party suppliers.

7. Service constraints

## 7.1. Maintenance Windows

Planned maintenance and upgrades are performed out of hours (18:00 – 08:00) or at weekends.

Any planned maintenance which must be completed during normal working hours will be notified to the customer at least 48 hours in advance.

## 7.2. Level of Customisation Permitted

The Verto application allows the Customer's Verto Administrators to customise the following elements:

- Number and Names of Gateways
- Gateway Navigation Items
- Navigation Item Fields
- Navigation Item Field Names
- Fields – Mandatory and / or Read Only
- Lookup Tables
- Tags
- User Permissions

The initial customisation is performed during the implementation stage by TMI working with the customer. Verto Administrator training covers all aspects of customisation allowing the administrator to make their own changes if required.

## 7.3. Schedule for deprecation of functionality/features

Each new release of Verto is supplied with a comprehensive list of functions that have been added/removed. Where it is the intention of TMI to deprecate a feature, the notification for this is published along with the release notes. Users have a minimum of 6 months to migrate data away from deprecated features.

**8. Service Levels**

## 8.1. Service Availability

Web Applications hosted by TMI Systems Ltd have a guaranteed uptime of 99% 24 x 7 x 365. The service availability of the Data Centre used by TMI Systems is 99.99% 24 x 7 x 365.

## 8.2. Support Hours

**Help Desk – 8:30 a.m. – 5:30 p.m. Monday – Friday**

Faults can be reported via email or phone and are logged on the TMI CRM system which allocates a unique reference and records the customer and individual raising the fault in addition to the description of the fault, etc.

Faults are given the highest priority and are aimed to be fixed within 60 minutes where possible.

This support is in place for as long as the customer has annual maintenance cover.

Requests for bug fixes, routine maintenance upgrades, 'legislative' upgrades, enhancements, release of new functionality are logged on the TMI CRM system which allocates a unique reference and can be made by email or phone.

Bug fixes, routine maintenance upgrades, and 'legislative' upgrades are released on a periodic basis and are all covered by the annual maintenance agreement.

Enhancements are collated and reviewed and if a request for functionality is unique to a customer, a quote for the work will be supplied. Where requests for enhancements are considered to be beneficial for other customers, these are added to the TMI log and scheduled for development. No charge is associated for these enhancements.

## 9. Financial recompense model for not meeting service levels

Our standard terms and conditions and service level agreement are enclosed. No formal compensation model exists in the event of service levels not being met. Any compensation would be agreed with the client on a case by case basis.

## 10. Training

Training is primarily focused using a "Train the Trainer' approach.  The standard training package consists of 3 modules:

**Module One**

The first training module delivered to system administrators is focused on the system *design and build process*. The module is delivered via two separate **online** sessions.

**Module Two**

The second training module delivered to system administrators is focused on the *system maintenance and management* processes. The module is delivered via two separate **online** sessions.

**Module Three**

The final training module delivered to system administrators is focused on *output reporting.* The module is delivered via two separate **online** sessions

Client organisations can request further training i.e., End User Training if this is beneficial to the implementation process.  Training is delivered on-line and tailored to the audience.

Training materials are provided as well as access to an easy-to-follow online resource area (The Knowledge Hub) containing guidance, articles and videos. Help and advice can be given to support any guidance notes that the client organisation may wish to produce. These documents can be stored in the generic Verto folder for easy access.

To assist end users with learning, within Verto, on-screen help and tips can be added either at screen level or at individual field level.  A link to the Knowledge Hub is also provided.

In addition, a newsletter is sent to Verto Administrators informing them of new upgrades.

11. Ordering and invoicing process
The Verto service is normally supplied on receipt of a Purchase Order or emailed order confirmation. Payment terms are 30 days following invoice.

12. Termination terms
The Verto service can be terminated at any time by the client. No specific notice period is required; terms and conditions and service level agreement are enclosed (Appendix A – TMI Systems Contract and Appendix B – TMI Systems SLA).

## 12.1. By consumers (i.e. consumption)
Should the service be terminated by either party, all client data will be returned directly.

Please also see section 4.2

## 12.2. By the Supplier (removal of the G-Cloud Service)
Should the service be terminated by either party, all client data will be returned directly

Please also see section 4.2

13. Data restoration / service migration
Wholesale restoration of a customer database has a target SLA of 4 hours, please see Appendix C - Verto Technical Platform. Where users request the restoration of individual data elements, the full audit capabilities of the application allow users to restore project data to any previous save point.

Where users are seeking to migrate away from the Verto service, the off-boarding process is followed see section 4.2 above.

14. Consumer responsibilities

Consumers should follow standard guidelines for Password Security and follow Data Protection guidelines.

15. Technical requirements

Please request Appendix C - Verto Technical Platform.

16. Details of any trial service available.

A 30-day free trial service is available via the website following registration for an online demonstration.

17. Specialist Cloud Services.

TMI Systems offer Verto software which is a hosted service (SaaS) and which can be used to manage work collaboration and project management across the organisation.

TMI Systems are also able to offer the following support services:

- Design Authority
- Project / Programme Management
- Business Analysis
- Design and Development
- Testing
- Project Specification and Selection
- Service Integration
- Deployment
- Transition Management (including rapid inter cloud service data/service migration)
- Service Management
- User Management
- Training
- Editorial

# Appendix A – TMI Systems Contract.

**AGREEMENT FOR THE SUPPLY OF SOFTWARE SOLUTIONS**

**Terms and Conditions for the supply of software to clients ("conditions")**

**1) Definitions**

1.1   "Project Specification" means a brief description of the work undertaken by TMI Systems Ltd and if the project will include milestones and payment upon completion of such milestones.

1.2   "Business Day" means any day which is not a Saturday, a Sunday or a public Holiday in England and Wales.

1.3   "TMI Systems" represents a partnership of fully qualified and diligent Information technology consultants.

1.4   "Client" means the person, firm, unincorporated association or corporate body to whom TMI Systems shall provide the specified software to.

1.5   "TMI Systems fees" means the sum payable to TMI Systems by the client for the agreed work in accordance with the applicable rates set out in the specification sheet, plus VAT where applicable.

1.6   "Contract" means the agreement relating to the provisions provided by TMI Systems to carry out the specified work to the named client.

**2) Contract**

2.1   This contract governs the agreement between TMI Systems Ltd and the named client (overleaf) hereby TMI Systems provides the client with the Specified software and or technological solutions.

2.2   No variation of or alteration to this contract shall be valid unless approved by a partner of TMI Systems in writing.

2.3   Unless otherwise agreed in writing by a partner of TMI Systems, this contract shall prevail over any terms of business or purchase conditions proffered by the client.

**3) Fees and Payment**

3.1   TMI Systems' fees are 100% to be paid on commencement of this agreement as signed for by both parties unless milestone payments have been specified and agreed to.

3.2   TMI Systems shall render invoices in accordance with the provisions of Clause 3.1

**4) Confidentiality**

4.1   In order to protect the confidentiality and trade secrets of TMI Systems and without prejudice to any other duty to keep secret information given to or gained by the client in confidence the client agrees –

(a)   Not at any time, whether during the said agreed work (unless expressly authorised by TMI Systems in writing or as otherwise required by law) to disclose to any other person or to make use of trade secrets or confidential information of TMI Systems or its associated companies other than in relation to any information which is deemed confidential or a trade secret and is already known to the client prior to the commencement of the said agreed work or which is already in the public domain;

4.2   In order to protect the confidentiality and trade secrets of the client and without prejudice to any other duty to keep secret information given to or gained by any TMI Systems consultant gained in confidence, TMI Systems shall procure that it's consultants shall agree:

(a)   Not at any time, whether during or after the said agreed work (unless expressly authorised by the client in writing or as otherwise required by law) to disclose to any person or to make use of the trade secrets or confidential information of the client or its associated companies other than in relation to any information which is deemed confidential or a trade secret and is already known to TMI Systems or a consultant prior to commencement of the said agreed work or which is already in the public domain.

**5) Copyright & Conditions of data**

5.1   All Intellectual property rights in the data contained in the service ('the data'), the software ('the software') and in any documentation accompanying the service ('the documentation') are owned by TMI Systems or its suppliers and is protected by copyright as in Copyright, designs and patents Act 1988. The "client" shall retain ownership at all times of data entered into and transferred into the "software".

5.2   All Intellectual property may only be accessed or distributed by the users specifically and expressly agreed by TMI Systems

5.3   TMI Systems reserve the right to retain all intellectual property rights as herein stated copyright of all software (including any images, "applets", photographs, animations, video, audio and text incorporated into the SOFTWARE) and database rights.

5.4    The client or any other persons may not rent, lease, transfer or distribute the SOFTWARE without expressed authorisation from TMI Systems.

5.5    TMI Systems are not responsible for the availability of access to our products and you are expected to ensure that your hardware and software if applicable are capable of effectively accessing the product and or services TMI Systems has provided. You are also advised to use appropriate anti-virus software where applicable before and during access to products and services.

5.6    In the unlikely event of insolvency as defined in *Insolvency Act 1986 as amended 1994* TMI Systems will transfer the intellectual property rights of the agreed specified SOFTWARE or database rights to the client.

5.7    The client, its employees, agents or any of their associates must take appropriate technical and organisational measures to protect the data against accidental or unlawful destruction and accidental loss and against unauthorised alteration or disclosure, or any other unauthorised form of processing.

5.8    TMI Systems are not liable whatsoever legally or otherwise for any consequential liability caused by use, misuse, loss, or theft within the system whether caused accidentally, unlawfully or negligently by the Client, its employees, agents or any of their associates.

5.9    The Client must provide a suitable level of security with respect to integrity, the nature of the data and the potential risks involved.

## 6) Liability

6.1    The following provisions set out the entire financial liability of TMI Systems (including liability for the acts or omissions of its consultants, or such other employees or agents) to the client in respect of any breach of these conditions and any representation, statement or tortious act or omission including negligence arising under or in connection with the contract or any work pursuant to the contract.

6.2    TMI Systems total aggregate liability in contract, tort (including negligence or breach of statutory duty) misrepresentation or otherwise, arising in connection with the performance or contemplated performance of this contract shall be limited to the total fees paid by the client to TMI Systems in respect of the work outlined in the project specification *only*; and

(a)    TMI Systems shall not be liable to the client for any indirect or consequential loss or damage (whether for loss of profit, loss of business, depletion of goodwill or otherwise), costs, expenses or other claims for consequential compensation whatsoever (howsoever caused)  which arise out of or in connection with the contract or any work pursuant to the contract.

6.3    The client hereby acknowledges and agrees that the limitation of liability set out herein in this clause 6 are reasonable and fair for a contract of this nature between the parties.

## 7) Restriction

7.1    This contract is personal to the client who may not assign it or any rights herein, or delegate or sub-contract the performance of any of its obligations hereunder, except as provided herein with TMI Systems's written permission.

7.2    This contract and the other documents referred to herein constitute the entire agreement between the parties relating to the transactions contemplated by this contract and supersede and extinguish all previous agreements, arrangements and undertakings between the parties in respect of the subject matter hereof.

7.3    The contract may be executed in either one or two counterparts, all of which taken together shall constitute one and the same instrument. The execution by a party of one or more counterparts shall constitute execution by that party of this contract for all purposes.

## 8) Force Majeure

8.1    If any party is totally or partially prevented or delayed in the performance of any of its obligations under the pursuant to this Agreement by force majeure and gives written notice thereof to the other party specifying the matters constituting force majeure and the period for which it is estimated that such prevention or delay will continue, together with such evidence as it is reasonably can give, the party so prevented or delayed shall allow a fair and reasonable extension for completion of this Agreement upon the happenings of any such event causing delay, if any circumstance arises which renders it impossible or illegal for either party to fulfil his contractual obligations, or if there is an outbreak of war then this agreement will be duly terminated.

8.2    In this agreement "Force majeure" shall mean any cause preventing either party from performing any or all of its obligations which arises from a or is attributable acts, events, omissions or accidents beyond the reasonable control of the party so prevented including without limitation strikes, lock-outs or other industrial disputes, act of God, war, riot, civil commotion, malicious damage, compliance with any law or government order, rule, regulation or direction, accident, breakdown of plant or machinery, telecommunications or utilities failure, fire or flood.

## 9) General Provisions

9.1    No waiver by either party of any breach of this Agreement shall be considered as a waiver of any subsequent breach of the same or any other term or condition.

9.2 If any provision of the Agreement is held by any competent authority to be invalid or unenforceable in whole or in part the validity of the other provisions of this contract and the remainder of the provisions in question shall not be affected thereby.

**10) Law**

    10.1    This contract shall be governed by English Law and the parties submit to the exclusive jurisdiction of the English courts.

# Appendix B – TMI Systems SLA



**tmi systems**                                               Service Level Agreement

## Software Service Level Agreement

This Service level agreement covers the provision of annual support and maintenance and annual hosting for the Verto Software as a Service application. "Initial Maintenance Period" means a fixed period of 12 months commencing on the date of activation of the Software to the Customer; "Extended Maintenance Period" means a recurring period of 12 months commencing on the day following the expiry of the Initial Maintenance Period ("the Commencement Date") and thereafter on the relevant anniversary of the Commencement Date;

"Maintenance Period" means the Extended Maintenance Period or the Initial Maintenance Period.

1.1 Subject to these terms and conditions and in consideration of the Agreement to supply software solutions by TMI Systems Ltd.

1.2 Subject to clauses 1.3 and 1.4, TMI Systems Ltd. shall provide and the Customer shall be obliged to pay the Maintenance Charge (as defined in Agreement to supply software solutions) and shall receive the Maintenance Services during the Extended Maintenance Period until the Customer gives notice to TMI Systems Ltd. as provided for in clause 1.4, subject always to the provisions for earlier termination provided in these terms and conditions.

1.3 Notwithstanding clause 1.2, TMI Systems Ltd. may elect not to provide the Maintenance Services during any Extended Maintenance Period by giving notice to the Customer not later than 60 days prior to the expiry of the previous Maintenance period.

1.4 The Customer may elect not to receive the Maintenance Services during any Extended Maintenance Period by giving notice to TMI Systems Ltd. not later than 60 days prior to the expiry of the previous maintenance period

1.5 For the avoidance of doubt, if the Customer does not give notice to TMI Systems Ltd. as provided for in clause 1.4 the Customer shall be invoiced for the provision of the Maintenance Services during the next Extended Maintenance Period in accordance with clause 1.8

1.6 The minimum cost per annum for the Maintenance Services during each Extended Maintenance Period ("the Maintenance Charge") shall be stated on the Agreement for the supply of software solutions. TMI Systems Ltd.shall in its discretion be entitled to increase the Maintenance Charge annually and the Maintenance Charge payable shall be the amount stipulated on the invoice issued in accordance with clause 1.8.

1.7 If TMI Systems Ltd wishes to increase the Maintenance Charge by more than 5%, it shall notify the Customer of its intention to make such a change not less than 30 days prior to the expiry of the preceding Extended Maintenance Period.

1.8 Unless notice is given by the Customer in accordance with clause 1.4 an invoice in respect of the Maintenance Charge will be issued in the month prior to the expiry of the Initial Maintenance Period or the preceding Extended Maintenance Period as appropriate. Payment of the Maintenance Charge shall be made to TMI Systems Ltd. without set off or counterclaim within 28 days of the date of the invoice.

## Annual Support and Maintenance

**Help Desk – 8:30 a.m. – 5:30 p.m. Monday – Friday** (excluding bank holidays)
**Tel: 0204 526 5925   email: support@vertocloud.co.uk**

Support questions can be reported via email or phone. Any calls or emails that cannot be immediately resolved are dealt with on a first come first served basis. Notification of the resolution will be set via email.

Faults (System Unavailable) are given the highest priority and are aimed to be fixed within 60 minutes where possible. The following table further outlines response times:

| Priority | Description / Nature | Initial Response | Target Resolution |
|---|---|---|---|
| P1 | System Unavailable or >75% of users unable to access. | 15 minutes | 1 Hour |
| P2 | Significant fault. Multiple users affected. System available but degraded. | 15 minutes | 4 Hours |
| P3 | Minor fault, e.g. display issues. | 20 minutes | 2 Days |
| P4 | Enhancement. Request for new functionality | 1 Hour | N/A |

**Upgrades**

Product upgrades will be available when new functionality is added to the software or new statutory requirements have been issued. These updates will be part of a controlled release procedure determined by TMI Systems and are covered by the annual support and maintenance fee

Where a request for enhanced or new functionality has been requested by a customer, TMI Systems Ltd. will endeavour to add this functionality to the standard product where appropriate.

The upgrades / enhancements will be distributed to all customers on our hosted platform at the same time and will not require end user intervention. Wherever possible, changes to the production platform are notified 7 days in advance. Sometimes for operational reasons (such as security patches, or system faults) it is necessary to change the production platform without notice – in this case users are notified retrospectively.

**Change Control Process**

In order to ensure that the TMI Systems Ltd. applications function as described, a Change Control process operates. A customer should contact TMI Systems Ltd with a request for a change to the existing functionality. The change could fall into one of three categories:
- Bug
- Enhancement
- New Functionality

As much detail as possible to support the request should be provided and any screen shots, etc, emailed to TMI Systems Ltd. On receipt, the request will be added to the TMI Systems Ltd. request list and a reference number will be allocated. All requests will be analysed to access any impact on the existing application.

An analysis of the request will be undertaken and, where a charge may be made for new functionality, this will be discussed with the customer prior to any work commencing. If the request is chargeable, on receipt of written approval, work will commence and the enhancement will be released in line with TMI Systems Ltd. procedures. Any bugs reported will follow the same procedure as above, but will be treated as the highest priority and fixed at zero cost.

All software updates are released to each client's Verto test site in the first instance prior to approval and release to their live site.

**Data, backups and return**

All customer data is stored within the EU and has a nightly backup cycle of 90 days. It is therefore possible for a customer to recover their data to the close of business on any day in the past 90 days. Client data can be returned within 7 days as a SQL server backup in the version of SQL server currently being used by the Verto platform.

**Service Availability**

Software as a Service Applications hosted by TMI Systems Ltd will have an uptime of 99.999% during core business hours (0900-1730 Mon-Fri). Outside of core business hours this service level drops to 99.8% to allow downtime for system upgrades. The service availability of the Data Centre used by TMI Systems is 99.999% 24 x 7 x 365.

**Appendix C – Verto Technical Platform.** Available on request.

# Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Platform 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:

## 1. Pricing Mechanism

1.1. All Charges under this Call-Off Contract will operate using a Time and Materials pricing mechanism.

## 2. Ordering

2.1. All payments will be made in accordance with the Call-Off Terms and Conditions and the Order Form, in particular the Payment Profile section.

2.2. Ahead of each Anniversary Date, the Buyer will confirm their volumes for the next Year and place an Order accordingly.

2.3. Any annual Charges for Services that are Ordered within a Year will be pro-rated to the next Anniversary Date.

2.4. Any one-off Charges for Services will be paid for upon Delivery, in line with the Payment Profile.

## 3. Charges relating to licences, hosting and support
The Buyer has the ability to call-off any of the Services detailed in the table below that relate to licences, hosting and support. The associated Charges for each item, applied on either a one-off or annual basis, is detailed for each Service:

| Charge Reference | Item | One-Off Charges | Annual Charges |
|---|---|---|---|
| C3.1 | Verto365 Pro Perpetual Licence | RE-DACTED | RE-DACTED |
| C3.2 | Verto365 Pro Annual Read Only Licence | RE-DACTED | RE-DACTED |
| C3.3 | Verto365 Pro Annual Timesheet Licence | RE-DACTED | RE-DACTED |
| C3.4 | Verto Workspaces (REDACTED) | RE-DACTED | RE-DACTED |
| C3.5 | Verto Workspaces Licences per user (RE-DACTED) | RE-DACTED | RE-DACTED |
| C3.6 | Annual Support and Maintenance (the units are as per the number of Verto365 Pro Perpetual Licences) | RE-DACTED | RE-DACTED |
| C3.7 | Annual Hosting (the units are as per the number of Verto365 Pro Perpetual Licences) | RE-DACTED | RE-DACTED |

## 4. Charges relating to other associated Services

The Buyer has the ability to call-off any of the Services detailed in the table below that relate to other associated Services.  The associated Charges for each item, applied on either a one-off or annual basis, is detailed for each Service:

| Charge Reference | Item | One-Off Charges |
|---|---|---|
| C4.1 | Installation and Setup for provisioning the System, which will only be incurred once at the start of the Term | RE-DACTED |
| C4.2 | Administrator Training Package | RE-DACTED |
| C4.3 | Call-off Day Rate for associated Services | RE-DACTED |
| C4.4 | Integration with Microsoft Teams and Single Sign On | RE-DACTED |

# Schedule 3: Collaboration agreement

Not used.

# Schedule 4: Alternative clauses

Not used.

## Schedule 5: Guarantee

Not used.

# Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

| Expression | Meaning |
|---|---|
| **Additional Services** | Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request. |
| **Admission Agreement** | The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s). |
| **Application** | The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform). |
| **Audit** | An audit carried out under the incorporated Framework Agreement clauses. |
| **Background IPRs** | For each Party, IPRs:<br>● 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<br>● created by the Party independently of this Call-Off Contract, or<br><br>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:<br>● 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<br>● other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential'). |
| **Control** | 'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly. |

| | |
|---|---|
| **Controller** | Takes the meaning given in the UK GDPR. |
| **Crown** | The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf. |

| | |
|---|---|
| **Data Loss Event** | Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach. |
| **Data Protection Impact Assessment (DPIA)** | An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data. |
| **Data Protection Legislation (DPL)** | (i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy. |
| **Data Subject** | Takes the meaning given in the UK GDPR |

| | |
|---|---|
| **Default** | Default is any:<br>● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)<br>● 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<br><br>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. |
| **DPA 2018** | Data Protection Act 2018. |
| **Employment Regulations** | The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE')         . |
| **End** | Means to terminate; and Ended and Ending are construed accordingly. |
| **Environmental Information Regulations or EIR** | The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations. |
| **Equipment** | The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract. |

| | |
|---|---|
| **ESI Reference Number** | The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool. |
| **Employment Status Indicator test tool or ESI tool** | The HMRC Employment Status Indicator test tool. The most up-todate version must be used. At the time of drafting the tool may be found here:<br>https://www.gov.uk/guidance/check-employment-status-fortax |
| **Expiry Date** | The expiry date of this Call-Off Contract in the Order Form. |

| | |
|---|---|
| **Force Majeure** | A force Majeure event means anything affecting either Party's performance of their obligations arising from any:<br>● acts, events or omissions beyond the reasonable control of the affected Party<br>● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare<br>● acts of government, local government or Regulatory Bodies<br>● fire, flood or disaster and any failure or shortage of power or fuel<br>● industrial dispute affecting a third party for which a substitute third party isn't reasonably available<br><br>The following do not constitute a Force Majeure event:<br>● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain<br>● 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<br>● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into<br>● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans |
| **Former Supplier** | A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor). |
| **Framework Agreement** | The clauses of framework agreement RM1557.13 together with the Framework Schedules. |

| | |
|---|---|
| **Fraud** | Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or |

| | |
|---|---|
| | defrauding or attempting to defraud or conspiring to defraud the Crown. |
| **Freedom of Information Act or FoIA** | The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation. |
| **G-Cloud Services** | The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement. |
| **UK GDPR** | The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679). |
| **Good Industry Practice** | Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances. |

| | |
|---|---|
| **Government Procurement Card** | The government's preferred method of purchasing and payment for low value goods or services. |
| **Guarantee** | 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: <br> ● a voluntary arrangement <br> ● a winding-up petition <br> ● the appointment of a receiver or administrator <br> ● an unresolved statutory demand <br> ● a Schedule A1 moratorium <br> ● a Dun & Bradstreet rating of 10 or less |
| **Intellectual Property Rights or IPR** | Intellectual Property Rights are: <br> ● 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 <br> ● 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 <br> ● all other rights having equivalent or similar effect in any country or jurisdiction <br><br> Perpetual licences can be reused by NHSBSA for external aswell as internal use, as authorised by the Verto Administrator at NHSBSA. |
| **Intermediary** | For the purposes of the IR35 rules an intermediary can be: <br> ● the supplier's own limited company <br> ● a service or a personal service company ● a partnership <br><br> 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 Buyer's possession before the Start date. |
| **Law** | Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply. |
| **Loss** | All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly. |
| **Lot** | Any of the 3 Lots specified in the ITT and Lots will be construed accordingly. |

| | |
|---|---|
| **Malicious Software** | Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence. |
| **Management Charge** | The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract. |
| **Management Information** | The management information specified in Framework Agreement Schedule 6. |
| **Material Breach** | Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract. |
| **Ministry of Justice Code** | The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000. |

| | |
|---|---|
| **New Fair Deal** | The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended. |

| | |
|---|---|
| **Order** | An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes. |
| **Order Form** | The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services. |
| **Ordered G-Cloud Services** | G-Cloud Services which are the subject of an order by the Buyer. |
| **Outside IR35** | Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool. |
| **Party** | The Buyer or the Supplier and 'Parties' will be interpreted accordingly. |
| **Personal Data** | Takes the meaning given in the UK GDPR. |

| | |
|---|---|
| **Personal Data Breach** | Takes the meaning given in the UK GDPR. |
| **Platform** | The government marketplace where Services are available for Buyers to buy. |
| **Processing** | Takes the meaning given in the UK GDPR. |
| **Processor** | Takes the meaning given in the UK GDPR. |
| **Prohibited act** | 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: <br>● induce that person to perform improperly a relevant function or activity <br>● reward that person for improper performance of a relevant function or activity <br>● commit any offence: ○ under the Bribery Act 2010 <br>    ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud <br>    ○ committing or attempting or conspiring to commit Fraud |

| | |
|---|---|
| **Project Specific IPRs** | Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs. |
| **Property** | Assets and property including technical infrastructure, IPRs and equipment. |
| **Protective Measures** | Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it. |
| **PSN or Public Services Network** | The Public Services Network (PSN) is the government's highperformance 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 GCloud Services, including backup data. |
| **Service definition(s)** | The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement. |
| **Service description** | The description of the Supplier service offering as published on the Platform. |
| **Service Personal Data** | The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract. |
| **Spend controls** | The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlsche ck-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 GCloud Services or any part thereof. |
| **Subcontractor** | Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services. |
| **Subprocessor** | Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract. |
| **Supplier** | The person, firm or company identified in the Order Form. |
| **Supplier Representative** | The representative appointed by the Supplier from time to time in relation to the Call-Off Contract. |

| | |
|---|---|
| **Supplier staff** | All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract. |
| **Supplier Terms** | The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application. |
| **Term** | The term of this Call-Off Contract as set out in the Order Form. |
| **Variation** | This has the meaning given to it in clause 32 (Variation process). |
| **Working Days** | Any day other than a Saturday, Sunday or public holiday in England and Wales. |
| **Year** | A contract year. |

# Schedule 7: UK GDPR Information

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

# Annex 1: Processing Personal Data

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

1.1        The contact details of the Buyer's Data Protection Officer are: Chris Gooday (chris.gooday@nhs.net).

1.2        The contact details of the Supplier's Data Protection Officer are: Ross Mardell (Ross.mardell@VertoCloud.co.uk)

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

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

| Description | Details |
| --- | --- |
| Identity of Controller for each Category of Personal Data | **The Buyer is Controller and the Supplier is Processor**<br><br>The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, Buyer is the Controller and the Supplier is the Processor of the Personal Data recorded below<br>Name and email address of system users only. |
| Duration of the Processing | Up to 7 years after the expiry or termination of the Framework Agreement |

| | |
|---|---|
| Nature and purposes of the Processing | To facilitate the fulfilment of the Supplier's obligations arising under this Framework Agreement including<br><br>    i.   Ensuring effective communication between the Supplier and CSS<br><br>    ii.  Maintaining full and accurate records ofevery Call-Off Contract arising under the<br>Framework Agreement in accordance with Clause 7.6 |
| Type of Personal Data | user name and email only |
| Categories of Data Subject | NHSBSA staff |
| Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data | All relevant data to be deleted 7 years after the expiry or termination of this Framework Contract unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder |

# Annex 2: Joint Controller Agreement

Not used