**Framework Schedule 6 (Order Form Template and Call-Off Schedules)**

**Order Form**

CALL-OFF REFERENCE: **K280022387**

THE BUYER: **Driver and Vehicle Standards Agency (DVSA)**

BUYER ADDRESS **Berkeley House**

**Croydon Street**

**Bristol**

**BS5 0DA**

THE SUPPLIER: Phoenix Software Ltd

SUPPLIER ADDRESS:Blenheim House, York Road, Pocklington, York,  
 YO42 1NS

REGISTRATION NUMBER:02548628

DUNS NUMBER: **76-348-8178**

SID4GOV ID: **76-348-8178**

This Order Form, when completed and executed by both Parties, forms a Call-Off Contract. A Call-Off Contract can be completed and executed using an equivalent document or electronic purchase order system.

If an electronic purchasing system is used instead of signing as a hard-copy, text below must be copied into the electronic order form

It is essential that if you, as the Buyer, add to or amend any aspect of any Call-Off Schedule, then **you must send the updated Schedule** with the Order Form to the Supplier

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 25th March 2025.

It’s issued under the Framework Contract with the reference number RM6098 for the provision of Technology Products & Associated Service 2.

CALL-OFF LOT(S):

Lot 3 Software

CALL-OFF INCORPORATED TERMS

This is a Gold Contract

The following documents are incorporated into this Call-Off Contract. Where numbers are missing, we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM6098
3. Framework Special Terms
4. The following Schedules in equal order of precedence:

* Joint Schedules for RM6098
  + Joint Schedule 2 (Variation Form)
  + Joint Schedule 3 (Insurance Requirements)
  + Joint Schedule 4 (Commercially Sensitive Information)
  + Joint Schedule 6 (Key Subcontractors)
  + Joint Schedule 7 (Financial Difficulties)
  + Joint Schedule 9 (Minimum Standards of Reliability)
  + Joint Schedule 10 (Rectification Plan)
  + Joint Schedule 11 (Processing Data)
  + Joint Schedule 12 (Supply Chain Visibility)
* Call-Off Schedules for RM6098
  + Call-Off Schedule 1 (Transparency Reports)
  + Call-Off Schedule 3 (Continuous Improvement)
  + Call-Off Schedule 5 (Pricing Details)
  + Call-Off Schedule 6 (ICT Services)
  + Call-Off Schedule 7 (Key Supplier Staff)
  + Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  + Call-Off Schedule 9 (Security)
  + Call-Off Schedule 10 (Exit Management)
  + Call-Off Schedule 11 (Installation Works)
  + Call-Off Schedule 12 (Clustering)
  + Call-Off Schedule 13 (Implementation Plan and Testing)
  + Call-Off Schedule 14 (Service Levels)
  + Call-Off Schedule 15 (Call-Off Contract Management)
  + Call-Off Schedule 16 (Benchmarking)
  + Call-Off Schedule 18 (Background Checks)
  + Call-Off Schedule 20 (Call-Off Specification)

1. CCS Core Terms (version 3.0.11) as amended by the Framework Award Form
2. Joint Schedule 5 (Corporate Social Responsibility) RM6098
3. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

**CALL-OFF SPECIAL TERMS**

Not Applicable

CALL-OFF START DATE: **31st March 2025**

CALL-OFF EXPIRY DATE: **30th March 2028**

CALL-OFF INITIAL PERIOD: **3 years with an option to extend for an additional year (3 + 1)**

**CALL-OFF DELIVERABLES**

The Suppliers Deliverables shall be the transaction of the procurement of software licences as required by the Buyer and the associated reporting and billing.

The Supplier shall have no liability and/or responsibility of the performance of the software supplied and the Buyer’s use of such software shall be subject to the applicable end use licence terms and conditions.

Please refer to Call-Off Schedule 20 (Call-Off Specification) for further details.

**LOCATION FOR DELIVERY**

All services will be delivered online via Microsoft Teams and email, unless otherwise agreed between both parties.

**DATES FOR DELIVERY**See details in Call-Off Schedule 13 (Implementation Plan & Testing)

**TESTING OF DELIVERABLES**N/A

**WARRANTY PERIOD**

Warranty for software shall be as set out in the applicable end user licence terms and conditions.

**MAXIMUM LIABILITY**

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **£9,500,000.00.**

**CALL-OFF CHARGES**

See details in Call-Off Schedule 5 (Pricing Details).

The maximum value of this contract is **£38,000,000.00** over 4 years, with no commitment to spend to total value.

The maximum for the initial 3 years of the contract is XXXXXX redacted under FOIA section 43**.**

**REIMBURSABLE EXPENSES**

Not applicable

**PAYMENT METHOD**

Payment will be made by BACS.

A Purchase Order (PO) number for this requirement will be provided to the supplier. The supplier must quote the PO number on all invoices, and these must be submitted directly to: [ssc.accountspayable@ubusinessservices.co.uk](https://encoded-592c9deb-987b-4562-aa3c-9fa3d37d83e9.uri/mailto%3assc.accountspayable%40ubusinessservices.co.uk%2520)

**BUYER’S INVOICE ADDRESS:**

Berkely House,  
Croydon Street,  
Bristol,  
BS5 0DA

**BUYER’S AUTHORISED REPRESENTATIVE**

XXXXXX redacted under FOIA section 40

XXXXXX redacted under FOIA section 40

XXXXXX redacted under FOIA section 40

XXXXXX redacted under FOIA section 40

**BUYER’S ENVIRONMENTAL POLICY**



If link is inaccessible externally, this policy is available upon request.

**BUYER’S SECURITY POLICY**

These can be found in the Security folder.

**SUPPLIER’S AUTHORISED REPRESENTATIVE**

XXXXXX redacted under FOIA section 40

XXXXXX redacted under FOIA section 40

XXXXXX redacted under FOIA section 40

XXXXXX redacted under FOIA section 40

**SUPPLIER’S CONTRACT MANAGER**

XXXXXX redacted under FOIA section 40

XXXXXX redacted under FOIA section 40

XXXXXX redacted under FOIA section 40

XXXXXX redacted under FOIA section 40

**PROGRESS REPORT FREQUENCY**

Monthly

**PROGRESS MEETING FREQUENCY**

Monthly

**KEY STAFF**

XXXXXX redacted under FOIA section 40

XXXXXX redacted under FOIA section 40

XXXXXX redacted under FOIA section 40

XXXXXX redacted under FOIA section 40

**KEY SUBCONTRACTOR(S)**

Not Applicable

**COMMERCIALLY SENSITIVE INFORMATION**

As identified within Joint Schedule 4.

**SERVICE CREDITS**

Not applicable

**ADDITIONAL INSURANCES**

Not applicable

**GUARANTEE**

Not applicable

**SOCIAL VALUE COMMITMENT**

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender)

**MODERN SLAVERY**

Upon award, the supplier agrees to submit a Modern Slavery Assessment Tool to work towards improving protections while reducing the risk of exploitation of workers within supply chains.

|  |  |  |  |
| --- | --- | --- | --- |
| **For and on behalf of the Supplier:** | | **For and on behalf of the Buyer:** | |
| Signature: | XXXXXX redacted under FOIA section 40 | Signature: | XXXXXX redacted under FOIA section 40 |
| Name: | XXXXXX redacted under FOIA section 40 | Name: | XXXXXX redacted under FOIA section 40 |
| Role: | XXXXXX redacted under FOIA section 40 | Role: | XXXXXX redacted under FOIA section 40 |
| Date: | 31/3/2025 | Date: | 31/1/2025 |

**Call-Off Schedule 1 (Transparency Reports)**

1.1 The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (<https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles>). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.

1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.

1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.

1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

**Annex A: List of Transparency Reports**

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | **Content** | **Format** | **Frequency** |
| Social Value | Performance against social value commitments as per the Social Value KPIs which have been structured around the Supplier’s Social Value tender response. | Excel (Other formats may be acceptable, subject to Buyer approval) | Social Value KPI 1 & 3 are quarterly.  Social Value KPI 2 is annually |

**Call-Off Schedule 3 (Continuous Improvement)**

Buyer’s Rights

The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

Supplier’s Obligations

The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer’s costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.

The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.

In addition to Paragraph 2.1, the Supplier shall produce at the start of each Contract Year a plan for improving the provision of Deliverables and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year (**"Continuous Improvement Plan"**) for the Buyer's Approval. The Continuous Improvement Plan must include, as a minimum, proposals:

identifying the emergence of relevant new and evolving technologies;

changes in business processes of the Supplier or the Buyer and ways of working that would provide cost savings and/or enhanced benefits to the Buyer (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);

new or potential improvements to the provision of the Deliverables including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Deliverables; and

measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives.

The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred (100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.

The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.

The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.

If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.

Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:

the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and

the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.

The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.

All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.

Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.

At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.

**Call-Off Schedule 4 (Call Off Tender)**

Not applicable.

**Call-Off Schedule 5 (Pricing Details)**

Phoenix’s pricing schedule submitted as part of the tender forms part of this contract.

**Call-Off Schedule 6 (ICT Services)**

1. **Definitions**
   1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

|  |  |
| --- | --- |
| "Buyer Property" | the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract; |
| "Buyer Software" | any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables; |
| "Buyer System" | the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables; |
| “Commercial off the shelf Software” or “COTS Software” | Non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms |
| “Core Network” | the provision of any shared central core network capability forming part of the overall Services delivered to the Buyer, which is not specific or exclusive to a specific Call-Off Contract, and excludes any configuration information specifically associated with a specific Call-Off Contract; |
| "Defect" | any of the following:   * 1. any error, damage or defect in the manufacturing of a Deliverable; or   2. any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or |
|  |  |
|  |  |
|  | * 1. any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or   2. any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract; |
| "Emergency Maintenance" | ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault; |
| "ICT Environment" | the Buyer System and the Supplier System; |
| "Licensed Software" | all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software; |
| "Maintenance Schedule" | has the meaning given to it in paragraph 8 of this Schedule; |
| "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; |
| "New Release" | an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item; |
| "Open Source Software" | computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge; |
| "Operating Environment" | means the Buyer System and any premises (including the Buyer Premises, the Supplier’s premises or third party premises) from, to or at which:  the Deliverables are (or are to be) provided; or  the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or  where any part of the Supplier System is situated; |
| "Permitted Maintenance" | has the meaning given to it in paragraph 8.2 of this Schedule; |
| "Quality Plans" | has the meaning given to it in paragraph 6.1 of this Schedule; |
| "Sites" | has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place; |
| "Software" | Specially Written Software COTS Software and non-COTS Supplier and third party Software; |
| "Software Supporting Materials" | has the meaning given to it in paragraph 9.1 of this Schedule; |
| "Source Code" | computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software; |
| "Specially Written Software" | any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR; |
|  |  |
| "Supplier System" | the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System); |
|  |  |

1. **When this Schedule should be used**
   1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT Services which are part of the Deliverables.
2. **Buyer due diligence requirements** 
   1. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;
      1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;
      2. operating processes and procedures and the working methods of the Buyer;
      3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and
      4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.
   2. The Supplier confirms that it has advised the Buyer in writing of:
      1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;
      2. the actions needed to remedy each such unsuitable aspect; and
      3. a timetable for and the costs of those actions.
3. **Licensed software warranty**
   1. The Supplier represents and warrants that:
      1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the Buyer which are necessary for the performance of the Supplier’s obligations under this Contract including the receipt of the Deliverables by the Buyer;
      2. all components of the Specially Written Software shall:
         1. be free from material design and programming errors;
         2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels) and Documentation; and
         3. not infringe any IPR.
4. **Provision of ICT Services**
   1. The Supplier shall:
      1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;
      2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;
      3. ensure that the Supplier System will be free of all encumbrances;
      4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;
      5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;
5. **Standards and Quality Requirements**
   1. The Supplier shall develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**")**.**
   2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.
   3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.
   4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:
      1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;
      2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and
      3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.
6. **ICT Audit**
   1. The Supplier shall allow any auditor access to the Supplier premises to:
      1. inspect the ICT Environment and the wider service delivery environment (or any part of them);
      2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;
      3. review the Supplier’s quality management systems including all relevant Quality Plans.
7. **Maintenance of the ICT Environment**
   1. If specified by the Buyer in the Order Form, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.
   2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (other than to the Core Network) (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.
   3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance, including to the Core Network.
   4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.
8. **Intellectual Property Rights in ICT**
   1. **Assignments granted by the Supplier: Specially Written Software** 
      1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:
         1. the Documentation, Source Code and the Object Code of the Specially Written Software; and
         2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").
      2. The Supplier shall:
         1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;
         2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and
         3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier’s Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier’s Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.
      3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.
   2. **Licences for non-COTS IPR from the Supplier and third parties to the Buyer**
      1. Unless the Buyer gives its Approval the Supplier must not use any:
9. of its own Existing IPR that is not COTS Software;
10. third party software that is not COTS Software
    * 1. Where the Buyer Approves the use of the Supplier’s Existing IPR that is not COTS Software the Supplier shall grants to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer’s (or, if the Buyer is a Central Government Body, any other Central Government Body’s) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Call Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.
      2. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:
         1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and
         2. only use such third party IPR as referred to at paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.
      3. Where the Supplier is unable to provide a license to the Supplier’s Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.
      4. The Supplier may terminate a licence granted under paragraph 9.2.1 by giving at least thirty (30) days’ notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.
    1. **Licenses for COTS Software by the Supplier and third parties to the Buyer**
       1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
       2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
       3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licencee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
       4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:
          1. will no longer be maintained or supported by the developer; or
          2. will no longer be made commercially available
    2. **Buyer’s right to assign/novate licences**
       1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 9.2 (to:
          1. a Central Government Body; or
          2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.
       2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 9.2.
    3. **Licence granted by the Buyer**
       1. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).
    4. **Open Source Publication**
       1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:
          1. suitable for publication by the Buyer as Open Source; and
          2. based on Open Standards (where applicable),

and the Buyer may, at its sole discretion, publish the same as Open Source.

* + 1. The Supplier hereby warrants that the Specially Written Software and the New IPR:
       1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;
       2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;
       3. do not contain any material which would bring the Buyer into disrepute;
       4. can be published as Open Source without breaching the rights of any third party;
       5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and
       6. do not contain any Malicious Software.
    2. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:
       1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and
       2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer’s ability to publish such other items or Deliverables as Open Source.
  1. **Malicious Software**
     1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.
     2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.
     3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.7.2 shall be borne by the Parties as follows:
        1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and
        2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

**Call-Off Schedule 7 (Key Supplier Staff)**

1.1 The Order Form lists the key roles (“**Key Roles**”) and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.

1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);

1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or

1.4.3 the person’s employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.

1.5 The Supplier shall:

1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;

1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff’s employment contract, this will mean at least three (3) Months’ notice;

1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and

1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.

1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

**Call-Off Schedule 8 (Business Continuity and Disaster Recovery)**

1. **Definitions**
   1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

|  |  |
| --- | --- |
| **“Annual Revenue”** | means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology:  figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and  where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date; |
| **“Appropriate Authority” or “Appropriate Authorities”** | means the Buyer and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team; |
| **“Associates”** | means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles; |
| **"BCDR Plan"** | has the meaning given to it in Paragraph 2.2 of this Schedule; |
| **"Business Continuity Plan"** | has the meaning given to it in Paragraph 2.3.2 of this Schedule; |
| **“Class 1 Transaction”** | has the meaning set out in the listing rules issued by the UK Listing Authority; |
| **“Control”** | the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “**Controls**” and “**Controlled**” shall be interpreted accordingly; |
| **“Corporate Change Event”** | means:   * + - 1. any change of Control of the Supplier or a Parent Undertaking of the Supplier;       2. any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Deliverables;       3. any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Deliverables;       4. a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc;       5. an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier;       6. payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period;       7. an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;       8. any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group;       9. the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or       10. any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales; |
| **“Critical National Infrastructure”** | means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:  major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or  significant impact on the national security, national defence, or the functioning of the UK; |
| **“Critical Service Contract”** | a service contract which the Buyer has categorised as a Gold Contract using the Cabinet Office Contract Tiering Tool or which the Buyer otherwise considers should be classed as a Critical Service Contract; |
| **“CRP Information”** | means, together, the:  Group Structure Information and Resolution Commentary; and  UK Public Sector and CNI Contract Information; |
| **“Dependent Parent Undertaking”** | means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into the Contract, including for the avoidance of doubt the provision of the Deliverables in accordance with the terms of the Contract; |
| **"Disaster"** | the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable); |
| **"Disaster Recovery Deliverables"** | the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster; |
| **"Disaster Recovery Plan"** | has the meaning given to it in Paragraph 2.3.3 of this Schedule; |
| **"Disaster Recovery System"** | the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster; |
| **“Group Structure Information and Resolution Commentary”** | means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 to 4 and Appendix 1 to Part B; |
| **“Parent Undertaking”** | has the meaning set out in section 1162 of the Companies Act 2006; |
| **“Public Sector Dependent Supplier”** | means a supplier where that supplier, or that supplier’s group has Annual Revenue of £50 million or more of which over 50% is generated from UK Public Sector Business; |
| **"Related Supplier"** | any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time; |
| **"Review Report"** | has the meaning given to it in Paragraph 6.3 of this Schedule; |
| **“Strategic Supplier”** | means those suppliers to government listed at  https://www.gov.uk/government/publications/strategic-suppliers; |
| **“Subsidiary Undertaking”** | has the meaning set out in section 1162 of the Companies Act 2006; |
| **“Supplier Group”** | means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings; |
| **"Supplier's Proposals"** | has the meaning given to it in Paragraph 6.3 of this Schedule; |
| **“UK Public Sector Business”** | means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations; and |
| **“UK Public Sector / CNI Contract Information”** | means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 to 4 and Appendix 2 of Part B; |

**Part A: BCDR Plan**

1. **BCDR Plan**
   1. The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.
   2. At least ninety (90) Working Days prior to the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer’s written approval a plan (a **“BCDR Plan”**), which shall detail the processes and arrangements that the Supplier shall follow to:
      1. ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and
      2. the recovery of the Deliverables in the event of a Disaster
   3. The BCDR Plan shall be divided into four sections:
      1. Section 1 which shall set out general principles applicable to the BCDR Plan;
      2. Section 2 which shall relate to business continuity (the **"Business Continuity Plan"**);
      3. Section 3 which shall relate to disaster recovery (the **"Disaster Recovery Plan"**); and
      4. Section 4 which shall relate to an Insolvency Event of the Supplier, and Key-Subcontractors and/or any Supplier Group member (the “**Insolvency Continuity Plan**”).
   4. Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
2. **General Principles of the BCDR Plan (Section 1)**
   1. Section 1 of the BCDR Plan shall:
      1. set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;
      2. provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;
      3. contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;
      4. detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;
      5. contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;
      6. contain a risk analysis, including:
         1. failure or disruption scenarios and assessments of likely frequency of occurrence;
         2. identification of any single points of failure within the provision of Deliverables and processes for managing those risks;
         3. identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and
         4. a business impact analysis of different anticipated failures or disruptions;
      7. provide for documentation of processes, including business processes, and procedures;
      8. set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;
      9. identify the procedures for reverting to "normal service";
      10. set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;
      11. identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan;
      12. provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer’s business continuity plans;
      13. set out how the business continuity and disaster recovery elements of the BCDR Plan link to the Insolvency Continuity Plan, and how the Insolvency Continuity Plan links to the business continuity and disaster recovery elements of the BCDR Plan;
      14. contain an obligation upon the Supplier to liaise with the Buyer and (at the Buyer’s request) any Related Supplier with respect to issues concerning insolvency continuity where applicable; and
      15. detail how the BCDR Plan links and interoperates with any overarching and/or connected insolvency continuity plan of the Buyer and any of its other Related Suppliers in each case as notified to the Supplier by the Buyer from time to time.
   2. The BCDR Plan shall be designed so as to ensure that:
      1. the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;
      2. the adverse impact of any Disaster is minimised as far as reasonably possible;
      3. it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and
      4. it details a process for the management of disaster recovery testing.
   3. The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.
   4. The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI’s) or Service levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.
3. **Business Continuity (Section 2)**
   1. The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:
      1. the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and
      2. the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.
   2. The Business Continuity Plan shall:
      1. address the various possible levels of failures of or disruptions to the provision of Deliverables;
      2. set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;
      3. specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI’s) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and
      4. set out the circumstances in which the Business Continuity Plan is invoked.
4. **Disaster Recovery (Section 3)**
   1. The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
   2. The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:
      1. loss of access to the Buyer Premises;
      2. loss of utilities to the Buyer Premises;
      3. loss of the Supplier's helpdesk or CAFM system;
      4. loss of a Subcontractor;
      5. emergency notification and escalation process;
      6. contact lists;
      7. staff training and awareness;
      8. BCDR Plan testing;
      9. post implementation review process;
      10. any applicable Performance Indicators (PI’s) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI’s) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;
      11. details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;
      12. access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and
      13. testing and management arrangements.
5. **Insolvency Continuity Plan (Section 4)**
   1. The Insolvency Continuity Plan shall be designed by the Supplier to permit continuity of the business operations of the Buyer supported by the Deliverables through continued provision of the Deliverables following an Insolvency Event of the Supplier, any Key Sub-contractor and/or any Supplier Group member with, as far as reasonably possible, minimal adverse impact.
   2. The Insolvency Continuity Plan shall include the following:
      1. communication strategies which are designed to minimise the potential disruption to the provision of the Deliverables, including key contact details in respect of the supply chain and key contact details for operational and contract Supplier Staff, Key Subcontractor personnel and Supplier Group member personnel;
      2. identification, explanation, assessment and an impact analysis of risks in respect of dependencies between the Supplier, Key Subcontractors and Supplier Group members where failure of those dependencies could reasonably have an adverse impact on the Deliverables;
      3. plans to manage and mitigate identified risks;
      4. details of the roles and responsibilities of the Supplier, Key Subcontractors and/or Supplier Group members to minimise and mitigate the effects of an Insolvency Event of such persons on the Deliverables;
      5. details of the recovery team to be put in place by the Supplier (which may include representatives of the Supplier, Key Subcontractors and Supplier Group members); and
      6. sufficient detail to enable an appointed insolvency practitioner to invoke the plan in the event of an Insolvency Event of the Supplier.
6. **Review and changing the BCDR Plan**
   1. The Supplier shall review the BCDR Plan:
      1. on a regular basis and as a minimum once every six (6) Months;
      2. within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 8; and
      3. where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer’s written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer’s approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer’s prior written approval.
   2. Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.
   3. The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.
   4. Following receipt of the Review Report and the Supplier’s Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
   5. The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier’s expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.
7. **Testing the BCDR Plan**
   1. The Supplier shall test the BCDR Plan:
      1. regularly and in any event not less than once in every Contract Year;
      2. in the event of any major reconfiguration of the Deliverables
      3. at any time where the Buyer considers it necessary (acting in its sole discretion).
   2. If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer’s requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.
   3. The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.
   4. The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.
   5. The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:
      1. the outcome of the test;
      2. any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and
      3. the Supplier's proposals for remedying any such failures.
   6. Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.
8. **Invoking the BCDR Plan**
   1. In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.
   2. The Insolvency Continuity Plan element of the BCDR Plan, including any linked elements in other parts of the BCDR Plan, shall be invoked by the Supplier:
      1. where an Insolvency Event of a Key Sub-contractor and/or Supplier Group member (other than the Supplier) could reasonably be expected to adversely affect delivery of the Deliverables; and/or
      2. where there is an Insolvency Event of the Supplier and the insolvency arrangements enable the Supplier to invoke the plan.
9. **Circumstances beyond your control**
   1. The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.
10. **Amendments to this Schedule in respect of Bronze Contracts**
    1. Where a Buyer’s Call-Off Contract is a Bronze Contract, if specified in the Order Form, the following provisions of this Call-Off Schedule 8, shall be disapplied in respect of that Contract:
       1. Paragraph 1.3.4 of Part A so that the BCDR plan shall only be required to be split into the three sections detailed in paragraphs 1.3.1 to 1.3.3 inclusive;
       2. Paragraphs 2.1.13 to 2.1.15 of Part A, inclusive;
       3. Paragraph 5 (Insolvency Continuity Plan) of Part A;
       4. Paragraph 8.2 of Part A; and
       5. The entirety of Part B of this Schedule.
    2. Where a Buyer’s Call-Off Contract is a Bronze Contract, if specified in the Order Form, the following definitions in Paragraph 1 of this Call-Off Schedule 8, shall be deemed to be deleted:
       1. Annual Review;
       2. Appropriate Authority or Appropriate Authorities;
       3. Associates;
       4. Class 1 Transaction;
       5. Control;
       6. Corporate Change Event;
       7. Critical National Infrastructure;
       8. Critical Service Contract;
       9. CRP Information;
       10. Dependent Parent Undertaking;
       11. Group Structure Information and Resolution Commentary;
       12. Parent Undertaking;
       13. Public Sector Dependent Supplier;
       14. Subsidiary Undertaking;
       15. Supplier Group;
       16. UK Public Sector Business; and
       17. UK Public Sector/CNI Contract Information.

**Part B: Corporate Resolution Planning**

1. **Service Status and Supplier Status**
   1. This Contract is a Critical Service Contract.
   2. The Supplier shall notify the Buyer in writing within 5 Working Days of the Effective Date and throughout the Call-Off Contract Period within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier.
2. **Provision of Corporate Resolution Planning Information**
   1. Paragraphs 2 to 4 of this Part B shall apply if the Contract has been specified as a Critical Service Contract under Paragraph 1.1 of this Part B or the Supplier is or becomes a Public Sector Dependent Supplier.
   2. Subject to Paragraphs 2.6, 2.10 and 2.11 of this Part B:
      1. where the Contract is a Critical Service Contract, the Supplier shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the Effective Date; and
      2. except where it has already been provided, where the Supplier is a Public Sector Dependent Supplier, it shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the date of the Appropriate Authority’s or Appropriate Authorities’ request.
   3. The Supplier shall ensure that the CRP Information provided pursuant to Paragraphs 2.2, 2.8 and 2.9 of this Part B:
      1. is full, comprehensive, accurate and up to date;
      2. is split into two parts:
         1. Group Structure Information and Resolution Commentary;
         2. UK Public Service / CNI Contract Information and is structured and presented in accordance with the requirements and explanatory notes set out at Annex I of the latest published version of the Resolution Planning Guidance published by the Cabinet Office Government Commercial Function and available at https://www.gov.uk/government/publications/the-outsourcingplaybook and contains the level of detail required (adapted as necessary to the Supplier’s circumstances);
      3. incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Appropriate Authority or Appropriate Authorities to understand and consider the information for approval;
      4. provides a clear description and explanation of the Supplier Group members that have agreements for goods, services or works provision in respect of UK Public Sector Business and/or Critical National Infrastructure and the nature of those agreements; and
      5. complies with the requirements set out at Appendix 1 (Group Structure Information and Resolution Commentary) and Appendix 2 (UK Public Sector / CNI Contract Information) respectively.
   4. Following receipt by the Appropriate Authority or Appropriate Authorities of the CRP Information pursuant to Paragraphs 2.2, 2.8 and 2.9 of this Part B, the Buyer shall procure that the Appropriate Authority or Appropriate Authorities shall discuss in good faith the contents of the CRP Information with the Supplier and no later than 60 days after the date on which the CRP Information was delivered by the Supplier either provide an Assurance to the Supplier that the Appropriate Authority or Appropriate Authorities approves the CRP Information or that the Appropriate Authority or Appropriate Authorities rejects the CRP Information.
   5. If the Appropriate Authority or Appropriate Authorities rejects the CRP Information:
      1. the Buyer shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Supplier in writing of its reasons for its rejection; and
      2. the Supplier shall revise the CRP Information, taking reasonable account of the Appropriate Authority’s or Appropriate Authorities’ comments, and shall re-submit the CRP Information to the Appropriate Authority or Appropriate Authorities for approval within 30 days of the date of the Appropriate Authority’s or Appropriate Authorities’ rejection. The provisions of paragraph 2.3 to 2.5 of this Part B shall apply again to any resubmitted CRP Information provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure under Clause 34 of the Core Terms at any time.
   6. Where the Supplier or a member of the Supplier Group has already provided CRP Information to a Department or the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that Department and the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid (which has the meaning in paragraph 2.7 below) on the date by which the CRP Information would otherwise be required, the Supplier shall not be required to provide the CRP Information under Paragraph 2.2 if it provides a copy of the Valid Assurance to the Appropriate Authority or Appropriate Authorities on or before the date on which the CRP Information would otherwise have been required.
   7. An Assurance shall be deemed Valid for the purposes of Paragraph 2.6 of this Part B if:
      1. the Assurance is within the validity period stated in the Assurance (or, if no validity period is stated, no more than 12 months has elapsed since it was issued and no more than 18 months has elapsed since the Accounting Reference Date on which the CRP Information was based); and
      2. no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if the Contract had then been in force) have occurred since the date of issue of the Assurance.
   8. If the Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 2.8.3 of this Part B its initial CRP Information) to the Appropriate Authority or Appropriate Authorities:
      1. within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 2.11 of this Part B) unless the Supplier is relieved of the consequences of the Financial Distress Event under Paragraph 7.1 of Joint Schedule 7 (Financial Distress) (if applicable);
      2. within 30 days of a Corporate Change Event unless not required pursuant to Paragraph 2.10;
      3. within 30 days of the date that:
         1. the credit rating(s) of each of the Supplier and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 2.10; or
         2. none of the credit rating agencies specified at Paragraph 2.10 hold a public credit rating for the Supplier or any of its Parent Undertakings; and
      4. in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Appropriate Authority (whichever is the earlier), unless:
         1. updated CRP Information has been provided under any of Paragraphs 2.8.1 2.8.2 or 2.8.3 since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 2.8.4; or
         2. unless not required pursuant to Paragraph 2.10.
   9. Where the Supplier is a Public Sector Dependent Supplier and the Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 2.8.1 to 2.8.4 of this Part B, the Supplier shall provide at the request of the Appropriate Authority or Appropriate Authorities and within the applicable timescales for each event as set out in Paragraph 2.8 (or such longer timescales as may be notified to the Supplier by the Buyer), the CRP Information to the Appropriate Authority or Appropriate Authorities.
   10. Where the Supplier or a Parent Undertaking of the Supplier has a credit rating of either:
       1. Aa3 or better from Moody’s;
       2. AA- or better from Standard and Poors;
       3. AA- or better from Fitch;

the Supplier will not be required to provide any CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Supplier is relieved of the consequences of the Financial Distress Event under Paragraph 7.1 of Annex 3 to Joint Schedule 7 (Financial Distress), if applicable) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 2.10, in which cases the Supplier shall provide the updated version of the CRP Information in accordance with paragraph 2.8.

* 1. Subject to Paragraph 4, where the Supplier demonstrates to the reasonable satisfaction of the Appropriate Authority or Appropriate Authorities that a particular item of CRP Information is highly confidential, the Supplier may, having orally disclosed and discussed that information with the Appropriate Authority or Appropriate Authorities, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Supplier shall promptly provide the relevant information to the Appropriate Authority or Appropriate Authorities to the extent required under Paragraph 2.8.

1. **Termination Rights**
   1. The Buyer shall be entitled to terminate the Contract if the Supplier is required to provide CRP Information under Paragraph 2 of this Part B and either:
      1. the Supplier fails to provide the CRP Information within 4 months of the Effective Date if this is a Critical Service Contract or otherwise within 4 months of the Appropriate Authority’s or Appropriate Authorities’ request; or
      2. the Supplier fails to obtain an Assurance from the Appropriate Authority or Appropriate Authorities within 4 months of the date that it was first required to provide the CRP Information under the Contract,

which shall be deemed to be an event to which Clause 10.4.1 of the Core Terms applies and Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply accordingly.

1. **Confidentiality and usage of CRP Information**
   1. The Buyer agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Supplier and/or Supplier Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality.
   2. Where the Appropriate Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier’s request, the Buyer shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Supplier containing terms no less stringent than those placed on the Buyer under paragraph 4.1 of this Part B and Clause 15 of the Core Terms.
   3. The Supplier shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Appropriate Authority or Appropriate Authorities pursuant to Paragraph 2 of this Part B subject, where necessary, to the Appropriate Authority or Appropriate Authorities entering into an appropriate confidentiality agreement in the form required by the third party.
   4. Where the Supplier is unable to procure consent pursuant to Paragraph 4.3 of this Part B, the Supplier shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by:
      1. redacting only those parts of the information which are subject to such obligations of confidentiality;
      2. providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:
         1. summarising the information;
         2. grouping the information;
         3. anonymising the information; and
         4. presenting the information in general terms
   5. The Supplier shall provide the Appropriate Authority or Appropriate Authorities with contact details of any third party which has not provided consent to disclose CRP Information where that third party is also a public sector body and where the Supplier is legally permitted to do so.

**Appendix 1: Group structure information and resolution commentary**

1. The Supplier shall:
   1. provide sufficient information to allow the Appropriate Authority to understand the implications on the Supplier Group’s UK Public Sector Business and CNI contracts listed pursuant to Appendix 2 if the Supplier or another member of the Supplier Group is subject to an Insolvency Event;
   2. ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Supplier Group; and
   3. provide full details of the importance of each member of the Supplier Group to the Supplier Group’s UK Public Sector Business and CNI contracts listed pursuant to Appendix 2 and the dependencies between each.

**Appendix 2: UK Public Sector / CNI Contract Information**

1. The Supplier shall:
   1. provide details of all agreements held by members of the Supplier Group where those agreements are for goods, services or works provision and:
      1. are with any UK public sector bodies including: central Government departments and their arms-length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police fire and rescue, education bodies and the devolved administrations;
      2. are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in paragraph 1.1.1 of this Appendix 2 and where the member of the Supplier Group is acting as a key sub-contractor under the agreement with the end recipient; or
      3. involve or could reasonably be considered to involve CNI;
   2. provide the Appropriate Authority with a copy of the latest version of each underlying contract worth more than £5m per contract year and their related key sub-contracts, which shall be included as embedded documents within the CRP Information or via a directly accessible link.

**Call-Off Schedule 10 (Exit Management)**

1. **Definitions**
   1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

|  |  |
| --- | --- |
| **“Core Network”** | the provision of any shared central core network capability forming part of the overall Services delivered to the Buyer, which is not specific or exclusive to a specific Call-Off Contract, and excludes any configuration information specifically associated with a specific Call-Off Contract; |
| **“Core Network Assets”** | the assets used in the provision of the Core Network; |
| **"Exclusive Assets"** | Supplier Assets used exclusively by the Supplier or a Key Subcontractor in the provision of the Deliverables; |
| **"Exit Information"** | has the meaning given to it in Paragraph 3.1 of this Schedule; |
| **"Exit Manager"** | the person appointed by each Party to manage their respective obligations under this Schedule; |
| **“Exit Plan”** | the plan produced and updated by the Supplier during the Initial Period in accordance with Paragraph 4 of this Schedule; |
| **"Net Book Value"** | the current net book value of the relevant Supplier Asset(s) calculated in accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice); |
| **"Non-Exclusive Assets"** | those Supplier Assets used by the Supplier or a Key Subcontractor in connection with the Deliverables but which are also used by the Supplier or Key Subcontractor for other purposes; |
| **"Registers"** | the register and configuration database referred to in Paragraph 2.2 of this Schedule; |
| **"Replacement Goods"** | any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party; |
| **"Replacement Services"** | any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those services are provided by the Buyer internally and/or by any third party; |
| **"Termination Assistance"** | the provision of any configuration information reasonably required to effect the implementation of the Replacement Services excluding the Core Network;  any activity required to facilitate the transition from the live operation of an existing Service to the live operation of a Replacement Service excluding the Core Network; and  c) the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice; |
| **"Termination Assistance Notice"** | has the meaning given to it in Paragraph 5.1 of this Schedule; |
| **"Termination Assistance Period"** | the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule; |
| **"Transferable Assets"** | Exclusive Assets which are capable of legal transfer to the Buyer; |
| **"Transferable Contracts"** | Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation, excluding such contracts relating to the Core Network; |
| **"Transferring Assets"** | has the meaning given to it in Paragraph 8.2.1 of this Schedule; |
| **"Transferring Contracts"** | has the meaning given to it in Paragraph 8.2.3 of this Schedule. |

1. **Supplier must always be prepared for contract exit** 
   1. The Supplier shall within 30 days from the Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.
   2. During the Contract Period, the Supplier shall promptly:
      1. create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and
      2. create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables

("**Registers**").

* 1. The Supplier shall:
     1. ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and
     2. procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.
  2. Each Party shall appoint an Exit Manager within three (3) Months of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

1. **Assisting re-competition for Deliverables** 
   1. The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "Exit Information").
   2. The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier’s or its Subcontractors’ prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.
   3. The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information (excluding the Core Network) which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).
   4. The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables (excluding the Core Network); and not be disadvantaged in any procurement process compared to the Supplier.
2. **Exit Plan**
   1. The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.
   2. The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
   3. The Exit Plan shall set out, as a minimum:
      1. a detailed description of both the transfer and cessation processes, including a timetable;
      2. how the Deliverables (excluding the Core Network) will transfer to the Replacement Supplier and/or the Buyer;
      3. details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;
      4. proposals for the training of key members of the Replacement Supplier’s staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;
      5. proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;
      6. proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;
      7. proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;
      8. proposals for the disposal of any redundant Deliverables and materials;
      9. how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and
      10. any other information or assistance reasonably required by the Buyer or a Replacement Supplier.
   4. The Supplier shall:
      1. maintain and update the Exit Plan (and risk management plan) no less frequently than:
         1. every six (6) months throughout the Contract Period; and
         2. no later than twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;
         3. as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than ten (10) Working Days after the date of the Termination Assistance Notice;
         4. as soon as reasonably possible following, and in any event no later than twenty (20) Working Days following, any material change to the Deliverables (including all changes under the Variation Procedure); and
      2. jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.
   5. Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.
   6. A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.
3. **Termination Assistance** 
   1. The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:
      1. the nature of the Termination Assistance required; and
      2. the start date and initial period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the End Date.
   2. The Buyer shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:
      1. no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and
      2. the Buyer shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.
   3. The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.
   4. Where the Buyer indicates in a Termination Assistance Notice that it requires any additional services to assist with exit in accordance with paragraph 5.1.3, the Supplier shall provide to the Buyer within ten (10) Working Days of receipt of such Termination Assistance Notice a quotation in the form of an itemised list of costs (in line with any day rates specified in the Contract) for each line of the additional services that the Buyer requires. Within five (5) Working Days of receipt of such quotation the Buyer shall confirm to the Supplier which of those itemised services it requires and the Supplier shall provide those services as part of the Termination Assistance at the Charges provided in the quotation
   5. In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).
4. **Termination Assistance Period** 
   1. Throughout the Termination Assistance Period the Supplier shall:
      1. continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;
      2. provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;
      3. use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;
      4. subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI’s) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;
      5. at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;
      6. seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.
   2. If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.
   3. If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.
5. **Obligations when the contract is terminated** 
   1. The Supplier shall comply with all of its obligations contained in the Exit Plan.
   2. Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:
      1. vacate any Buyer Premises;
      2. remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;
      3. provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:
         1. such information relating to the Deliverables as remains in the possession or control of the Supplier; and
         2. such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.
   3. Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.
6. **Assets, Sub-contracts and Software**
   1. Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:
      1. terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or
      2. terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables excluding the Core Network; or
      3. (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.
   2. Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:
      1. which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("Transferring Assets");
      2. which, if any, of:
         1. the Exclusive Assets that are not Transferable Assets; and
         2. the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

* + 1. which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the **"Transferring Contracts"**),

in order for the Buyer and/or its Replacement Supplier to provide the Deliverables excluding the Core Network from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables (excluding the Core Network) or the Replacement Goods and/or Replacement Services (excluding the Core Network).

* 1. With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.
  2. Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.
  3. Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:
     1. procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which
     2. procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.
  4. The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.
  5. The Buyer shall:
     1. accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and
     2. once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.
  6. The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.
  7. The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

1. **No charges** 
   1. Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.
2. **Dividing the bills** 
   1. All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:
      1. the amounts shall be annualised and divided by 365 to reach a daily rate;
      2. the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and
      3. the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

**Call-Off Schedule 11 (Installation Works)  
*Not applicable currently, but before use, this schedule has to be approved by both parties***

**When this Schedule should be used**

This Schedule is designed to provide additional provisions necessary to facilitate the provision of Deliverables requiring installation by the Supplier.

**How things must be installed**

Where the Supplier reasonably believes, it has completed the Installation Works it shall notify the Buyer in writing. Following receipt of such notice, the Buyer shall inspect the Installation Works and shall, by giving written notice to the Supplier:

accept the Installation Works, or

reject the Installation Works and provide reasons to the Supplier if, in the Buyer’s reasonable opinion, the Installation Works do not meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract).

If the Buyer rejects the Installation Works in accordance with Paragraph 2.1.2, the Supplier shall immediately rectify or remedy any defects and if, in the Buyer’s reasonable opinion, the Installation Works do not, within five (5) Working Days of such rectification or remedy, meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract), the Buyer may terminate this Contract for material Default.

The Installation Works shall be deemed to be completed when the Supplier receives a notice issued by the Buyer in accordance with Paragraph 2.2.1 Notwithstanding the acceptance of any Installation Works in accordance with Paragraph 2.2), the Supplier shall remain solely responsible for ensuring that the Goods and the Installation Works conform to the specification in the Call-Off Order Form (or elsewhere in this Contract). No rights of estoppel or waiver shall arise as a result of the acceptance by the Buyer of the Installation Works.

Throughout the Contract Period, the Supplier shall have at all times all licences, approvals and consents necessary to enable the Supplier and the Supplier Staff to carry out the Installation Works.

**Call-Off Schedule 12 (Clustering)**

***Not applicable currently, but before use, this schedule has to be approved by both parties***

**When you should use this Schedule**

This Schedule is required where various Other Contracting Authorities want to join with the Buyer to efficiently contract collectively under a single Call Off Contract rather than as separate individual Buyers under separate Call Off Contracts.

**Definitions**

**“Cluster Members"** means a person named as such in the Annex A to this Schedule which shall be incorporated into the Order Form.

**Cluster Members benefits under the Contract**

The Buyer has entered into this Call-Off Contract both for its own benefit and for the benefit the Cluster Members.

The Cluster Members who are to benefit under the Call-Off Contract are identified Annex 1 to this Schedule which shall be included into Order Form.

Cluster Members shall have all of the rights granted to the Buyer under a Call-Off Contract. Accordingly, where the context requires in order to assure the Cluster Members rights and benefits under a Call-Off Contract, and unless the Buyer otherwise specifies, references to the Buyer in a Call-Off Contract (including those references to a Party which are intended to relate to the Buyer) shall be deemed to include a reference to the Cluster Members.

Each of the Cluster Members will be a third party beneficiary for the purposes of the CRTPA and may enforce the relevant provisions of a Call-Off Contract pursuant to CRTPA.

The Parties to a Call-Off Contract may in accordance with its provisions vary, terminate or rescind that Call-Off Contract or any part of it, without the consent of any Cluster Member.

The enforcement rights granted to Cluster Members under Paragraph 1.4 are subject to the following provisions:

the Buyer may enforce any provision of a Call-Off Contract on behalf of a Cluster Member;

any claim from a Cluster Member under the CRTPA to enforce a Call-Off Contract shall be brought by the Buyer if reasonably practicable for the Buyer and Cluster Member to do so; and

the Supplier's limits and exclusions of liability in the Call-Off Contract shall apply to any claim to enforce a Call-Off Contract made by the Buyer on behalf of a Cluster Member and to any claim to enforce a Call-Off Contract made by a Cluster Member acting on its own behalf.

Notwithstanding that Cluster Members shall each receive the same Services from the Supplier the following adjustments will apply in relation to how the Call-Off Contract will operate in relation to the Buyer and Cluster Members:

Services will be provided by the Supplier to each Cluster Member and Buyer separately;

the Supplier's obligation in regards to reporting will be owed to each Cluster Member and Buyer separately;

the Buyer and Cluster Members shall be entitled to separate invoices in respect of the provision of Deliverables;

the separate invoices will correlate to the Deliverables provided to the respective Buyer and Cluster Members;

the Charges to be paid for the Deliverables shall be calculated on a per Cluster Member and Buyer basis and each Cluster Member and the Buyer shall be responsible for paying their respective Charges;

the Service Levels and corresponding Service Credits will be calculated in respect of each Cluster Member and Buyer, and they will be reported and deducted against Charges due by each respective Cluster Member and Buyer; and

such further adjustments as the Buyer and each Cluster Member may notify to the Supplier from time to time.

**Annex A – Cluster Members**

The Deliverables shall also be provided for the benefit of the following Cluster Members:

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Cluster Member | Services to be provided | Duration | Special Terms |
| [ ] | [ ] | [ ] | [ ] |
| [ ] | [ ] | [ ] | [ ] |
| [ ] | [ ] | [ ] | [ ] |
| [ ] | [ ] | [ ] | [ ] |

**Call-Off Schedule 13 (Implementation Plan and Testing)**

***Not applicable currently, but before use, this schedule has to be approved by both parties***

Part A - Implementation

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Delay" a) a delay in the Achievement of a Milestone by its Milestone Date; or

b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;

"Deliverable Item" an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan;

"Milestone Payment" a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone;

Implementation Period" has the meaning given to it in Paragraph 7.1;

2. Agreeing and following the Implementation Plan

2.1 A draft of the Implementation Plan is set out in the Annex to this Schedule. The Supplier shall provide a further draft Implementation Plan 30 days after the Call-Off Contract Start Date.

2.2 The draft Implementation Plan:

2.2.1 must contain information at the level of detail necessary to manage the implementation stage effectively and as the Buyer may otherwise require; and

2.2.2 it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.

2.3 Following receipt of the draft Implementation Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the Implementation Plan. If the Parties are unable to agree the contents of the Implementation Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

2.4 The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is Achieved on or before its Milestone Date.

2.5 The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.

3. Reviewing and changing the Implementation Plan

3.1 Subject to Paragraph 4.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer’s instructions and ensure that it is updated on a regular basis.

3.2 The Buyer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

3.3 Changes to any Milestones, Milestone Payments and Delay Payments shall only be made in accordance with the Variation Procedure.

3.4 Time in relation to compliance with the Implementation Plan shall be of the essence and failure of the Supplier to comply with the Implementation Plan shall be a material Default.

4. Security requirements before the Start Date

4.1 The Supplier shall note that it is incumbent upon them to understand the lead-in period for security clearances and ensure that all Supplier Staff have the necessary security clearance in place before the Call-Off Start Date. The Supplier shall ensure that this is reflected in their Implementation Plans.

4.2 The Supplier shall ensure that all Supplier Staff and Subcontractors do not access the Buyer's IT systems, or any IT systems linked to the Buyer, unless they have satisfied the Buyer's security requirements.

4.3 The Supplier shall be responsible for providing all necessary information to the Buyer to facilitate security clearances for Supplier Staff and Subcontractors in accordance with the Buyer's requirements.

4.4 The Supplier shall provide the names of all Supplier Staff and Subcontractors and inform the Buyer of any alterations and additions as they take place throughout the Call-Off Contract.

4.5 The Supplier shall ensure that all Supplier Staff and Subcontractors requiring access to the Buyer Premises have the appropriate security clearance. It is the Supplier's responsibility to establish whether or not the level of clearance will be sufficient for access. Unless prior approval has been received from the Buyer, the Supplier shall be responsible for meeting the costs associated with the provision of security cleared escort services.

4.6 If a property requires Supplier Staff or Subcontractors to be accompanied by the Buyer’s Authorised Representative, the Buyer must be given reasonable notice of such a requirement, except in the case of emergency access.

5. What to do if there is a Delay

5.1 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:

5.1.1 notify the Buyer as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;

5.1.2 include in its notification an explanation of the actual or anticipated impact of the Delay;

5.1.3 comply with the Buyer’s instructions in order to address the impact of the Delay or anticipated Delay; and

5.1.4 use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

6. Compensation for a Delay

6.1 If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Supplier shall pay to the Buyer such Delay Payments (calculated as set out by the Buyer in the Implementation Plan) and the following provisions shall apply:

6.1.1 the Supplier acknowledges and agrees that any Delay Payment is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier’s failure to Achieve the corresponding Milestone;

6.1.2 Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier’s failure to Achieve a Milestone by its Milestone Date except where:

(a) the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (When CCS or the Buyer can end this contract); or

(b) the delay exceeds the number of days (the "Delay Period Limit") specified in the Implementation Plan commencing on the relevant Milestone Date;

6.1.3 the Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is Achieved;

6.1.4 no payment or other act or omission of the Buyer shall in any way affect the rights of the Buyer to recover the Delay Payments or be deemed to be a waiver of the right of the Buyer to recover any such damages; and

6.1.5 Delay Payments shall not be subject to or count towards any limitation on liability set out in Clause 11 (How much you can be held responsible for).

7. Implementation Plan

7.1 The Implementation Period will be a six (6) Month period.

7.2 During the Implementation Period, the incumbent supplier shall retain full responsibility for all existing services until the Call-Off Start Date or as otherwise formally agreed with the Buyer. The Supplier's full service obligations shall formally be assumed on the Call-Off Start Date as set out in Order Form.

7.3 In accordance with the Implementation Plan, the Supplier shall:

7.3.1 work cooperatively and in partnership with the Buyer, incumbent supplier, and other Framework Supplier(s), where applicable, to understand the scope of Services to ensure a mutually beneficial handover of the Services;

7.3.2 work with the incumbent supplier and Buyer to assess the scope of the Services and prepare a plan which demonstrates how they will mobilise the Services;

7.3.3 liaise with the incumbent Supplier to enable the full completion of the Implementation Period activities; and

7.3.4 produce a Implementation Plan, to be agreed by the Buyer, for carrying out the requirements within the Implementation Period including, key Milestones and dependencies.

7.4 The Implementation Plan will include detail stating:

7.4.1 how the Supplier will work with the incumbent Supplier and the Buyer Authorised Representative to capture and load up information such as asset data ; and

7.4.2 a communications plan, to be produced and implemented by the Supplier, but to be agreed with the Buyer, including the frequency, responsibility for and nature of communication with the Buyer and end users of the Services.

7.5 In addition, the Supplier shall:

7.5.1 appoint a Supplier Authorised Representative who shall be responsible for the management of the Implementation Period, to ensure that the Implementation Period is planned and resourced adequately, and who will act as a point of contact for the Buyer;

7.5.2 mobilise all the Services specified in the Specification within the Call-Off Contract;

7.5.3 produce a Implementation Plan report for each Buyer Premises to encompass programmes that will fulfil all the Buyer's obligations to landlords and other tenants:

(a) the format of reports and programmes shall be in accordance with the Buyer's requirements and particular attention shall be paid to establishing the operating requirements of the occupiers when preparing these programmes which are subject to the Buyer's approval; and

(b) the Parties shall use reasonable endeavours to agree the contents of the report but if the Parties are unable to agree the contents within twenty (20) Working Days of its submission by the Supplier to the Buyer, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

7.5.4 manage and report progress against the Implementation Plan;

7.5.5 construct and maintain a Implementation risk and issue register in conjunction with the Buyer detailing how risks and issues will be effectively communicated to the Buyer in order to mitigate them;

7.5.6 attend progress meetings (frequency of such meetings shall be as set out in the Order Form) in accordance with the Buyer's requirements during the Implementation Period. Implementation meetings shall be chaired by the Buyer and all meeting minutes shall be kept and published by the Supplier; and

7.5.7 ensure that all risks associated with the Implementation Period are minimised to ensure a seamless change of control between incumbent provider and the Supplier.

Annex 1: Implementation Plan

The Implementation Plan is set out below and the Milestones to be Achieved are identified below:

Planned Action Deliverable Items Duration Milestone Date

Work with incumbent supplier to transfer current licences over Transfer of licences and agreements 7 days 1st April

The Milestones will be Achieved in accordance with this Call-Off Schedule 13: (Implementation Plan and Testing)

For the purposes of Paragraph 9.1.2 the Delay Period Limit shall be 7

Part B - Testing

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Component" any constituent parts of the Deliverables;

"Material Test Issue" a Test Issue of Severity Level 1 or Severity Level 2;

"Satisfaction Certificate" a certificate materially in the form of the document contained in Annex 2 issued by the Buyer when a Deliverable and/or Milestone has satisfied its relevant Test Success Criteria;

"Severity Level" the level of severity of a Test Issue, the criteria for which are described in Annex 1;

"Test Issue Management Log" a log for the recording of Test Issues as described further in Paragraph 8.1 of this Schedule;

"Test Issue Threshold" in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan;

"Test Reports" the reports to be produced by the Supplier setting out the results of Tests;

"Test Specification" the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph 6.2 of this Schedule;

"Test Strategy" a strategy for the conduct of Testing as described further in Paragraph 3.2 of this Schedule;

"Test Success Criteria" in relation to a Test, the test success criteria for that Test as referred to in Paragraph 5 of this Schedule;

"Test Witness" any person appointed by the Buyer pursuant to Paragraph 9 of this Schedule; and

"Testing Procedures" the applicable testing procedures and Test Success Criteria set out in this Schedule.

2. How testing should work

2.1 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, Test Specification and the Test Plan.

2.2 The Supplier shall not submit any Deliverable for Testing:

2.2.1 unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;

2.2.2 until the Buyer has issued a Satisfaction Certificate in respect of any prior, dependant Deliverable(s); and

2.2.3 until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).

2.3 The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.

2.4 Prior to the issue of a Satisfaction Certificate, the Buyer shall be entitled to review the relevant Test Reports and the Test Issue Management Log.

3. Planning for testing

3.1 The Supplier shall develop the final Test Strategy as soon as practicable after the Start Date but in any case no later than twenty (20) Working Days after the Start Date.

3.2 The final Test Strategy shall include:

3.2.1 an overview of how Testing will be conducted in relation to the Implementation Plan;

3.2.2 the process to be used to capture and record Test results and the categorisation of Test Issues;

3.2.3 the procedure to be followed should a Deliverable fail a Test, fail to satisfy the Test Success Criteria or where the Testing of a Deliverable produces unexpected results, including a procedure for the resolution of Test Issues;

3.2.4 the procedure to be followed to sign off each Test;

3.2.5 the process for the production and maintenance of Test Reports and a sample plan for the resolution of Test Issues;

3.2.6 the names and contact details of the Buyer and the Supplier's Test representatives;

3.2.7 a high level identification of the resources required for Testing including Buyer and/or third party involvement in the conduct of the Tests;

3.2.8 the technical environments required to support the Tests; and

3.2.9 the procedure for managing the configuration of the Test environments.

4. Preparing for Testing

4.1 The Supplier shall develop Test Plans and submit these for Approval as soon as practicable but in any case no later than twenty (20) Working Days prior to the start date for the relevant Testing as specified in the Implementation Plan.

4.2 Each Test Plan shall include as a minimum:

4.2.1 the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being Tested and, for each Test, the specific Test Success Criteria to be satisfied; and

4.2.2 a detailed procedure for the Tests to be carried out.

4.3 The Buyer shall not unreasonably withhold or delay its approval of the Test Plan provided that the Supplier shall implement any reasonable requirements of the Buyer in the Test Plan.

5. Passing Testing

5.1 The Test Success Criteria for all Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 4.

6. How Deliverables will be tested

6.1 Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least 10 Working Days prior to the start of the relevant Testing (as specified in the Implementation Plan).

6.2 Each Test Specification shall include as a minimum:

6.2.1 the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Buyer and the extent to which it is equivalent to live operational data;

6.2.2 a plan to make the resources available for Testing;

6.2.3 Test scripts;

6.2.4 Test pre-requisites and the mechanism for measuring them; and

6.2.5 expected Test results, including:

(a) a mechanism to be used to capture and record Test results; and

(b) a method to process the Test results to establish their content.

7. Performing the tests

7.1 Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.

7.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 9.3.

7.3 The Supplier shall notify the Buyer at least 10 Working Days in advance of the date, time and location of the relevant Tests and the Buyer shall ensure that the Test Witnesses attend the Tests.

7.4 The Buyer may raise and close Test Issues during the Test witnessing process.

7.5 The Supplier shall provide to the Buyer in relation to each Test:

7.5.1 a draft Test Report not less than 2 Working Days prior to the date on which the Test is planned to end; and

7.5.2 the final Test Report within 5 Working Days of completion of Testing.

7.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:

7.6.1 an overview of the Testing conducted;

7.6.2 identification of the relevant Test Success Criteria that have/have not been satisfied together with the Supplier's explanation of why any criteria have not been met;

7.6.3 the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;

7.6.4 the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in each case grouped by Severity Level in accordance with Paragraph 8.1; and

7.6.5 the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.

7.7 When the Supplier has completed a Milestone it shall submit any Deliverables relating to that Milestone for Testing.

7.8 Each party shall bear its own costs in respect of the Testing. However, if a Milestone is not Achieved the Buyer shall be entitled to recover from the Supplier, any reasonable additional costs it may incur as a direct result of further review or re-Testing of a Milestone.

7.9 If the Supplier successfully completes the requisite Tests, the Buyer shall issue a Satisfaction Certificate as soon as reasonably practical following such successful completion. Notwithstanding the issuing of any Satisfaction Certificate, the Supplier shall remain solely responsible for ensuring that the Deliverables are implemented in accordance with this Contract.

8. Discovering Problems

8.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.

8.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Buyer upon request.

8.3 The Buyer shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

9. Test witnessing

9.1 The Buyer may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Buyer, each of whom shall have appropriate skills to fulfil the role of a Test Witness.

9.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.

9.3 The Test Witnesses:

9.3.1 shall actively review the Test documentation;

9.3.2 will attend and engage in the performance of the Tests on behalf of the Buyer so as to enable the Buyer to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;

9.3.3 shall not be involved in the execution of any Test;

9.3.4 shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;

9.3.5 may produce and deliver their own, independent reports on Testing, which may be used by the Buyer to assess whether the Tests have been Achieved;

9.3.6 may raise Test Issues on the Test Issue Management Log in respect of any Testing; and

9.4 may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

10. Auditing the quality of the test

10.1 The Buyer or an agent or contractor appointed by the Buyer may perform on-going quality audits in respect of any part of the Testing (each a "Testing Quality Audit") subject to the provisions set out in the agreed Quality Plan.

10.2 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.

10.3 The Buyer will give the Supplier at least 5 Working Days' written notice of the Buyer’s intention to undertake a Testing Quality Audit.

10.4 The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Buyer to enable it to carry out the Testing Quality Audit.

10.5 If the Testing Quality Audit gives the Buyer concern in respect of the Testing Procedures or any Test, the Buyer shall prepare a written report for the Supplier detailing its concerns and the Supplier shall, within a reasonable timeframe, respond in writing to the Buyer’s report.

10.6 In the event of an inadequate response to the written report from the Supplier, the Buyer (acting reasonably) may withhold a Satisfaction Certificate until the issues in the report have been addressed to the reasonable satisfaction of the Buyer.

11. Outcome of the testing

11.1 The Buyer will issue a Satisfaction Certificate when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.

11.2 If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Buyer shall notify the Supplier and:

11.2.1 the Buyer may issue a Satisfaction Certificate conditional upon the remediation of the Test Issues;

11.2.2 the Buyer may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or

11.2.3 where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Buyer’s other rights and remedies, such failure shall constitute a material Default.

11.3 The Buyer shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.

11.4 The Buyer shall issue a Satisfaction Certificate in respect of a given Milestone as soon as is reasonably practicable following:

11.4.1 the issuing by the Buyer of Satisfaction Certificates and/or conditional Satisfaction Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and

11.4.2 performance by the Supplier to the reasonable satisfaction of the Buyer of any other tasks identified in the Implementation Plan as associated with that Milestone.

11.5 The grant of a Satisfaction Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of any Implementation Plan and Clause 4 (Pricing and payments).

11.6 If a Milestone is not Achieved, the Buyer shall promptly issue a report to the Supplier setting out the applicable Test Issues and any other reasons for the relevant Milestone not being Achieved.

11.7 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Buyer shall issue a Satisfaction Certificate.

11.8 If there is one or more Material Test Issue(s), the Buyer shall refuse to issue a Satisfaction Certificate and, without prejudice to the Buyer’s other rights and remedies, such failure shall constitute a material Default.

11.9 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Buyer may at its discretion (without waiving any rights in relation to the other options) choose to issue a Satisfaction Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:

11.9.1 any Rectification Plan shall be agreed before the issue of a conditional Satisfaction Certificate unless the Buyer agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Buyer within 10 Working Days of receipt of the Buyer’s report pursuant to Paragraph 10.5); and

11.9.2 where the Buyer issues a conditional Satisfaction Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

12. Risk

12.1 The issue of a Satisfaction Certificate and/or a conditional Satisfaction Certificate shall not:

12.1.1 operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Buyer’s requirements for that Deliverable or Milestone; or

12.1.2 affect the Buyer’s right subsequently to reject all or any element of the Deliverables and/or any Milestone to which a Satisfaction Certificate relates.

Annex 1: Test Issues – Severity Levels

1. Severity 1 Error

1.1 This is an error that causes non-recoverable conditions, e.g. it is not possible to continue using a Component.

2. Severity 2 Error

2.1 This is an error for which, as reasonably determined by the Buyer, there is no practicable workaround available, and which:

2.1.1 causes a Component to become unusable;

2.1.2 causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or

2.1.3 has an adverse impact on any other Component(s) or any other area of the Deliverables;

3. Severity 3 Error

3.1 This is an error which:

3.1.1 causes a Component to become unusable;

3.1.2 causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or

3.1.3 has an impact on any other Component(s) or any other area of the Deliverables;

but for which, as reasonably determined by the Buyer, there is a practicable workaround available;

4. Severity 4 Error

4.1 This is an error which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Deliverables.

5. Severity 5 Error

5.1 This is an error that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Deliverables.

Annex 2: Satisfaction Certificate

To: [insert name of Supplier]

From: [insert name of Buyer]

[insert Date dd/mm/yyyy]

Dear Sirs,

Satisfaction Certificate

Deliverable/Milestone(s): [Insert relevant description of the agreed Deliverables/Milestones].

We refer to the agreement ("Call-Off Contract") [insert Call-Off Contract reference number] relating to the provision of the [insert description of the Deliverables] between the [insert Buyer name] ("Buyer") and [insert Supplier name] ("Supplier") dated [insert Call-Off Start Date dd/mm/yyyy].

The definitions for any capitalised terms in this certificate are as set out in the Call-Off Contract.

[We confirm that all the Deliverables relating to [insert relevant description of Deliverables/agreed Milestones and/or reference number(s) from the Implementation Plan] have been tested successfully in accordance with the Test Plan [or that a conditional Satisfaction Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria].

[OR]

[This Satisfaction Certificate is granted on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with Clause 4 (Pricing and payments)].

Yours faithfully

[insert Name]

[insert Position]

acting on behalf of [insert name of Buyer]

**Call-Off Schedule 14 (Service Levels)**

1. **Definitions**
   1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

|  |  |
| --- | --- |
| **“Critical Service Level Failure”** | has the meaning given to it in the Order Form; |
| **"Service Credits"** | 1. any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels; |
| **"Service Credit Cap"** | 1. has the meaning given to it in the Order Form; |
|  |  |
| **"Service Level Failure"** | 1. means a failure to meet the Service Level Performance Measure in respect of a Service Level; |
| **"Service Level Performance Measure"** | 1. shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and |
| **"Service Level Threshold"** | 1. shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule. |

1. **What happens if you don’t meet the Service Levels**
   1. The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.
   2. The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier’s failure to meet any Service Level Performance Measure.
   3. The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.
   4. A Service Credit shall be the Buyer’s exclusive financial remedy for a Service Level Failure except where:
      1. the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or
      2. the Service Level Failure:
         1. exceeds the relevant Service Level Threshold;
         2. has arisen due to a Prohibited Act or wilful Default by the Supplier;
         3. results in the corruption or loss of any Government Data; and/or
         4. results in the Buyer being required to make a compensation payment to one or more third parties; and/or
      3. the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).
   5. Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months’ notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:
      1. the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;
      2. the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and
      3. there is no change to the Service Credit Cap.
2. **Critical Service Level Failure**

On the occurrence of a Critical Service Level Failure:

* 1. any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and
  2. the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"),

provided that the operation of this paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

**Part A: Service Levels and Service Credits**

1. **Service Levels**

If the level of performance of the Supplier:

* 1. is likely to or fails to meet any Service Level Performance Measure; or
  2. is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

* + 1. require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;
    2. instruct the Supplier to comply with the Rectification Plan Process;
    3. if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or
    4. if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

1. **Service Credits**
   1. Not used

**Annex A to Part A: Services Levels and Service Credits Table**

| Service Levels | | |  |  |  | Service Credit for each Service Period |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Service Level Performance Criterion | Key Indicator | Service Level Performance Measure – Good > | Approaching target > | Requires Improvement > | Inadequate <= | Publishable KPI |
| Quotes for Software Licencing and Maintenance Support | Upon request of a quote for software by the Authority the Potential Provider must provide a quote and an indictive lead time within a period of 5 working days for standard items. | 98% | 89.9% | N/A | < 89.9% | N/A | No |
| Complex Software Requirements | Upon request of a quote for complex software by the Authority the Potential Provider must provide a quote and an indictive lead time within a period of 7 working days for anything complex. | Within 7 days 98% | N/A | N/A | Over 7 days = < 89.9% | N/A | Yes |
| Unable to procure via Reseller | Upon request of a quote for software by the Authority, where the reseller will not work with Potential Provider, the Potential Provider must advise the Authority within 20 days of receiving the quote request, to allow the Authority to manage the procurement. | Within 20 working days = 100% | Within 30 working days = 90% | N/A | Over 30 working days =  < 90% | N/A | Yes |
| Software Procured, Licences and EULA | Provide licence details and EULA following confirmation that the order has been placed with the reseller within 7 working days | Within 7 working days = 100% | Within 10 working days = 90% | N/A | Over 10 working days < 90% | N/A | No |
| Escalations/Refunds | Where a Vendor has not delivered on the requirement. Escalations/Refunds to be executed within 30 working days | Within 30 working days = 99% | N/A | N/A | Over 30 working days = < 89.9% | N/A | No |
| Communicating Changes | Provide advice on how they will communicate changes i.e. Licence metrics, license bundles, version configurations, pricing or user rights and any implications of those changes to licence terms and conditions to the Authority within 5 days of changes being announced. | Within 5 working days = 99% | N/A | N/A | Over 5 working days = < 89.9% | N/A | Yes |
| Review True-Up Licensing | Where true up licensing requirements are needed, a full review every 12 months with the option to true down is required. Subject to any re-strictions by Microsoft for the relevant products | Annual true up completed = 98% | N/A | N/A | True Ups not completed in line with anniversary dates = < 89.9% | N/A | No |
| Carbon Net Zero | Quarterly progress report to include  Total emissions (baseline and current)  Percentage reduction achieved  Comparison against targets  Key initiatives implemented  Any deviations from the plan and corrective actions | 99% | 89.9% | N/A | < 89.9% | N/A | No |
| Social Value 1 | To measure the contribution of apprenticeships towards social value creation, including skills development, employability, and community impact.   * Total number of apprenticeships offered during the reporting period. | 10 apprenticeships = 100% | 8 apprenticeships =  89.9% | 5 or under apprenticeships = 50% | 0 apprenticeships = 0% | N/A | No |
| Social Value 2 | To measure the contribution of apprenticeships towards social value creation, including skills development, employability, and community impact.   * Completion rate of apprenticeship programs and securing full-time employment within six months. | 99% | 89.9% | N/A | N/A |  | No |
| Social Value 3 | Proving reports in line with your Social Value bid to include:   * STEM Events * Providing an opportunity for the local communities and schools to discover new career paths in IT * Supporting the Manchester Skills City Bootcamp initiative * Apprenticeship scheme | All points covered within the report = 99% | Three out of four of the bullet points covered in the report = 89.9% | N/A | No report produced = 70% |  | Yes |

**Part B: Performance Monitoring**

1. **Performance Monitoring and Performance Review**
   1. Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.
   2. The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the process and timescales agreed pursuant to paragraph 1.1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:
      1. for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;
      2. a summary of all failures to achieve Service Levels that occurred during that Service Period;
      3. details of any Critical Service Level Failures;
      4. for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;
      5. the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and
      6. such other details as the Buyer may reasonably require from time to time.
   3. The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:
      1. take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;
      2. be attended by the Supplier's Representative and the Buyer’s Representative; and
      3. be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer’s Representative and any other recipients agreed at the relevant meeting.
   4. The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer’s Representative at each meeting.
   5. The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.
2. **Satisfaction Surveys**
   1. The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

**Call-Off Schedule 15 (Call-Off Contract Management)**

# Project Management

## The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

1. **Role of the Supplier Contract Manager**
   1. The Supplier's Contract Manager's shall be:

### the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;

### able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;

### able to cancel any delegation and recommence the position himself; and

### replaced only after the Buyer has received notification of the proposed change.

* 1. The Buyer may provide revised instructions to the Supplier's Contract Manager's in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.
  2. Receipt of communication from the Supplier's Contract Manager's by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

# Role of the Operational Board

## not used

1. **Contract Risk Management**
   1. Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.
   2. The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

### the identification and management of risks;

* + 1. the identification and management of issues; and
    2. monitoring and controlling project plans.
  1. The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.
  2. The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer's and the Supplier have identified.

**Annex: Contract Boards**

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

The contract management boards will be facilitated via Teams. However, some in person contract management boards at the DVSA and Phoenix sites or permitted.

**Call-Off Schedule 16 (Benchmarking)  
*Not applicable currently, but before use, this schedule has to be approved by both parties***

**DEFINITIONS**

In this Schedule, the following expressions shall have the following meanings:

|  |  |
| --- | --- |
| **"Benchmark Review"** | a review of the Deliverables carried out in accordance with this Schedule to determine whether those Deliverables represent Good Value; |
| **"Benchmarked Deliverables"** | any Deliverables included within the scope of a Benchmark Review pursuant to this Schedule; |
| **"Comparable Rates"** | the Charges for Comparable Deliverables; |
| **"Comparable Deliverables"** | deliverables that are identical or materially similar to the Benchmarked Deliverables (including in terms of scope, specification, volume and quality of performance) provided that if no identical or materially similar Deliverables exist in the market, the Supplier shall propose an approach for developing a comparable Deliverables benchmark; |
| **"Comparison Group"** | a sample group of organisations providing Comparable Deliverables which consists of organisations which are either of similar size to the Supplier or which are similarly structured in terms of their business and their service offering so as to be fair comparators with the Supplier or which, are best practice organisations; |
| **"Equivalent Data"** | data derived from an analysis of the Comparable Rates and/or the Comparable Deliverables (as applicable) provided by the Comparison Group; |
| **"Good Value"** | that the Benchmarked Rates are within the Upper Quartile; and |
| **"Upper Quartile"** | in respect of Benchmarked Rates, that based on an analysis of Equivalent Data, the Benchmarked Rates, as compared to the range of prices for Comparable Deliverables, are within the top 25% in terms of best value for money for the recipients of Comparable Deliverables. |

**When you should use this Schedule**

The Supplier acknowledges that the Buyer wishes to ensure that the Deliverables, represent value for money to the taxpayer throughout the Contract Period.

This Schedule sets to ensure the Contracts represent value for money throughout and that the Buyer may terminate the Contract by issuing a Termination Notice to the Supplier if the Supplier refuses or fails to comply with its obligations as set out in Paragraphs 3 of this Schedule.

Amounts payable under this Schedule shall not fall with the definition of a Cost.

**Benchmarking**

**How benchmarking works**

The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

The Buyer may, by written notice to the Supplier, require a Benchmark Review of any or all of the Deliverables.

The Buyer shall not be entitled to request a Benchmark Review during the first six (6) Month period from the Contract Commencement Date or at intervals of less than twelve (12) Months after any previous Benchmark Review.

The purpose of a Benchmark Review will be to establish whether the Benchmarked Deliverables are, individually and/or as a whole, Good Value.

The Deliverables that are to be the Benchmarked Deliverables will be identified by the Buyer in writing.

Upon its request for a Benchmark Review the Buyer shall nominate a benchmarker. The Supplier must approve the nomination within ten (10) Working Days unless the Supplier provides a reasonable explanation for rejecting the appointment.  If the appointment is rejected then the Buyer may propose an alternative benchmarker. If the Parties cannot agree the appointment within twenty (20) days of the initial request for Benchmark review then a benchmarker shall be selected by the Chartered Institute of Financial Accountants.

The cost of a benchmarker shall be borne by the Buyer (provided that each Party shall bear its own internal costs of the Benchmark Review) except where the Benchmark Review demonstrates that the Benchmarked Service and/or the Benchmarked Deliverables are not Good Value, in which case the Parties shall share the cost of the benchmarker in such proportions as the Parties agree (acting reasonably). Invoices by the benchmarker shall be raised against the Supplier and the relevant portion shall be reimbursed by the Buyer.

**Benchmarking Process**

The benchmarker shall produce and send to the Buyer, for Approval, a draft plan for the Benchmark Review which must include:

a proposed cost and timetable for the Benchmark Review;

a description of the benchmarking methodology to be used which must demonstrate that the methodology to be used is capable of fulfilling the benchmarking purpose; and

a description of how the benchmarker will scope and identify the Comparison Group.

The benchmarker, acting reasonably, shall be entitled to use any model to determine the achievement of value for money and to carry out the benchmarking.

The Buyer must give notice in writing to the Supplier within ten (10) Working Days after receiving the draft plan, advising the benchmarker and the Supplier whether it Approves the draft plan, or, if it does not approve the draft plan, suggesting amendments to that plan (which must be reasonable). If amendments are suggested then the benchmarker must produce an amended draft plan and this Paragraph 3.2.3 shall apply to any amended draft plan.

Once both Parties have approved the draft plan then they will notify the benchmarker. No Party may unreasonably withhold or delay its Approval of the draft plan.

Once it has received the Approval of the draft plan, the benchmarker shall:

finalise the Comparison Group and collect data relating to Comparable Rates. The selection of the Comparable Rates (both in terms of number and identity) shall be a matter for the Supplier's professional judgment using:

market intelligence;

the benchmarker’s own data and experience;

relevant published information; and

pursuant to Paragraph 3.2.6 below, information from other suppliers or purchasers on Comparable Rates;

by applying the adjustment factors listed in Paragraph 3.2.7 and from an analysis of the Comparable Rates, derive the Equivalent Data;

using the Equivalent Data, calculate the Upper Quartile;

determine whether or not each Benchmarked Rate is, and/or the Benchmarked Rates as a whole are, Good Value.

The Supplier shall use all reasonable endeavours and act in good faith to supply information required by the benchmarker in order to undertake the benchmarking. The Supplier agrees to use its reasonable endeavours to obtain information from other suppliers or purchasers on Comparable Rates.

In carrying out the benchmarking analysis the benchmarker may have regard to the following matters when performing a comparative assessment of the Benchmarked Rates and the Comparable Rates in order to derive Equivalent Data:

the contractual terms and business environment under which the Comparable Rates are being provided (including the scale and geographical spread of the customers);

exchange rates;

any other factors reasonably identified by the Supplier, which, if not taken into consideration, could unfairly cause the Supplier's pricing to appear non-competitive.

**Benchmarking Report**

For the purposes of this Schedule **"Benchmarking Report"** shall mean the report produced by the benchmarker following the Benchmark Review and as further described in this Schedule;

The benchmarker shall prepare a Benchmarking Report and deliver it to the Buyer, at the time specified in the plan Approved pursuant to Paragraph 3.2.3, setting out its findings. Those findings shall be required to:

include a finding as to whether or not a Benchmarked Service and/or whether the Benchmarked Deliverables as a whole are, Good Value;

if any of the Benchmarked Deliverables are, individually or as a whole, not Good Value, specify the changes that would be required to make that Benchmarked Service or the Benchmarked Deliverables as a whole Good Value; and

include sufficient detail and transparency so that the Party requesting the Benchmarking can interpret and understand how the Supplier has calculated whether or not the Benchmarked Deliverables are, individually or as a whole, Good Value.

The Parties agree that any changes required to this Contract identified in the Benchmarking Report shall be implemented at the direction of the Buyer in accordance with Clause 24 (Changing the contract)

**Call-Off Schedule 18 (Background Checks)**

**When you should use this Schedule**

This Schedule should be used where Supplier Staff must be vetted before working on Contract.

**Definitions**

**“Relevant Conviction”** means any conviction listed in Annex 1 to this Schedule.

**Relevant Convictions**

The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.

Notwithstanding Paragraph 3.1.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):

carry out a check with the records held by the Department for Education (DfE);

conduct thorough questioning regarding any Relevant Convictions; and

ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),

and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

**Annex 1 – Relevant Convictions**

**N/A**

**Call-Off Schedule 18 (Background Checks)**

**When you should use this Schedule**

This Schedule should be used where Supplier Staff must be vetted before working on Contract.

**Definitions**

**“Relevant Conviction”** means any conviction listed in Annex 1 to this Schedule.

**Relevant Convictions**

The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.

Notwithstanding Paragraph 3.1.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):

carry out a check with the records held by the Department for Education (DfE);

conduct thorough questioning regarding any Relevant Convictions; and

ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),

and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

**Annex 1 – Relevant Convictions**

**N/A**

**Call-Off Schedule 20 (Call-Off Specification)**

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract

## The requirement

* 1. DVSA are looking for a Value-Added Reseller who will help source a variety of software licences while also proving a value-added service.
  2. At a high level, the service can be split into two main areas:
     1. **Non-Microsoft Software;** Procurement of all software that is not purchased via Government Procurement Card or relates to Microsoft but not limited to; end user software; enterprise software; developer software; specialist software and assistive technology.
     2. **Microsoft Software;** Procurement of all Microsoft related software.

* 1. **Microsoft requirements:**
     1. The Potential Provider must be able to provide various Microsoft software licences and a Microsoft Enterprise Agreement plus the provision of Microsoft Azure Cloud Hosting.
     2. The Potential Provider must align a dedicated resource to support the Microsoft Contract
     3. The Potential Provider must have Dynamics specific technical ability or have a 3rd Party as part of being our Microsoft partner to also assist with support and with any migration to any new licencing model.
     4. The Potential Provider to provide expertise in Microsoft, including but not limited to server, cloud, enterprise, dynamics as and when required and provide support and guidance on the following portals, Power Platform, Admin Centre, Visual Studio where appropriate. Surfacing options to enable an informed choice - across contract types, license metrics, editions versions and bundles that apply, ensuring use rights applicable are made visible, and finally pricing applicable to those options.  
          
        To Providing visibility of changes - notifying the right person, role or team as Microsoft change license metrics, product make up (e.g. taking capability out of a bundle or moving capability up to a premium edition), or prices.
     5. The agreement will allow the buyer to true up licensing requirements where needed and undertake a full review every 12 months with the option to true down if required.  Subject to any restrictions by Microsoft for the relevant products

* + 1. The Potential Provider will be required to confirm their tender submissions include access to the Microsoft Admin Centre (MAC) which provides access to download products and keys, access to Licencing information, relationship summary and licence summary details, status of enrolments and activation of Software Assurance Benefits.
    2. Potential Provider to provide Annual Licence Rationalisation Process to ensure the Microsoft licensing is compliant and optimal operational functionality.   Potential Provide to provide a SOW 90 days of the agreement anniversary.
    3. The Potential Provider is encouraged to engage with the Authority in events and forums where vendors such as Microsoft, release new products which can improve productivity or efficiency of the Authority demonstrating added value.
    4. Potential Provider should provide 3 days of free professional service consultancy for Microsoft associated products and subscriptions, as and when new products are released and/or when requested.
    5. Potential Provider to provide free 1–2-hour overview to the Software Asset Management Team on the MS Admin, CSP and Azure Portal. Advising what we can/should be able to see and utilise to our benefit every 6 months when requested.
    6. Potential Provider to carry out a free of charge preliminary Microsoft Health Check at the Anniversary of the contract.
    7. Potential Provider to provide a Free of Charge Cloud Enablement Workshop during the contract period, to provide value added services in relation to cloud support/advice. Workshops to include, but not limited to:
* Verify the health of our environment
* Improve organisational security
* Receive ideas to improve user adoption
* Meet compliancy
* Increase Productivity
* The aim is to identify cost savings by optimally licencing the agreement

* + 1. Potential Provider to provide Free of Charge Cloud Enablement Workshops to provide value added services in relation to cloud support/advice. Workshops to include, but not limited to;
* Advice and guidance on Azure, M365 or Microsoft Stack technologies
* Digital workshops, and technology strategy planning
* Cloud spend review
* Licencing review
* Quarterly technology workshops
* Technology webinars/podcasts

* 1. **The following covers both Microsoft and non-Microsoft:**
     1. Due to the high value nature of this contract, the Authority is requesting an open book contract. There will be no commitment to spend the full value of this contract.
     2. This requirements document and the Potential Provider’s response to this invitation to tender will make up the scope of service, and not be superseded by any statement of works or similar created during the transition stage. Changes to the service can be agreed via a contract change control process with agreement of both the Potential Provider and the Authority.
     3. The Potential Provider must align a dedicated Account Manager and Licencing specialist as well as an alternative contact as an escalation route for this contract.
     4. The Authority reserves the right to seek all services listed in this statement of requirement elsewhere without prior consultation of the Potential Provider.
     5. The Potential Provider will support the Authority on achieving the best lead times as set out in the SLA table (see section 5 of this document).
     6. The Potential Provider must be approved resellers/partners in order for the Authority to ensure it is achieving best value and kept up to speed with the latest developments.
     7. There is no guarantee that all current procured licences will be required/renewed moving forwards.
     8. The Potential Provider must be able to continue the Annual Billing for any software that has been procured prior to this contract being in place.
     9. The Potential Provider must provide a continuous delivery model which should be implemented allowing rapid ROI and value realisation, delivering strategic solutions using Agile/DevOps methodologies.
     10. The Authority reserve the right to carry out ad hoc audits direct with the Potential Provider to check that markups are within the agreed limits.
     11. All quotes MUST include the period and our Reference Number (which will be on the title of the email request).
     12. The Potential Provider must provide confirmation that the order is in place and provide copies of licence/software documentation e.g. EULAs, Licence Keys on completion of the order and sent to the shared mailbox together with the contract period and quoting our Reference Number.
     13. The Potential Provider must be able to demonstrate they have provided best value for money and can meet any seasonal demands
     14. The Potential Provider must provide the Authority with advice on how they will communicate changes i.e. Licence metrics, license bundles, version configurations, pricing or user rights and any implications of those changes to licence terms and conditions to the Authority, within 5 working days of changes being announced.
     15. The Potential Provider will arrange any training with the software provider and liaise with the relevant Authorities Teams to provide the necessary training requirements/dates/periods. i.e. assistive training when purchased as part of the software requirements or when part of a project when the authority are looking for a particular software requirement.
     16. The Potential Provider must be able to provide ITSM and Sec Ops Managed Service Support and assist the Agency with identifying the most suitable ITSM platform based on our requirements when requested and provide a SOW detailing the requirements with associated fees
     17. The Potential Provider must provide a breakdown or an accessible Dashboard that provides the following sub totalled by month, as per example below at the Service and Contract Board Meetings (see section 7).
     18. Potential partner should be an Amazon Web Services Channel Partner who can provide CPPO (Channel Partner Private Offer) through Amazon Marketplace using the DVSA AWS ID associated with OGVA 2.0.
     19. Potential Provider to pay for all costs if a decision is made to integrate with our ITSM Tool.

## Management information/reporting

* 1. The Potential Provider shall work with the Authority to ensure adequate service review mechanisms are put in place. This will require the Potential Provider to assign a dedicated account manager who will be required to attend DVSA sites periodically.

* 1. A services review will be held monthly to assess Potential Provider’s performance against SLAs, as well as discuss any outstanding issues and agree actions to resolve.
  2. Monthly Contract Reviews will take place particularly in the first year. For these reviews the Potential Provider will provide a written report, this report will contain details of the total spend per month under the contract which the report relates.
  3. The Supplier’s performance will be managed using Key Performance Indicators (KPIs) and Service Levels. The KPIs and Service Levels will be recorded within the statement of requirement and Call Off Order Form. These will be monitored regularly throughout the contract term.
  4. As this requirement is for an overarching licence provider captured in the statement of requirement, the KPIs and Service Levels will reflect this. There will be overarching KPIs/Service Levels which will be monitored frequently throughout the contract term, and those specific to the SoWs which will have a reporting frequency agreed as part of the statement of requirement.
  5. Should the Authority request a supply chain map, the Winning Supplier is responsible for putting this together and presenting it at the Contract Management Boards when requested.
  6. Quotes that are sent through must include the level of discount the Authority are receiving (if appliable).

## 3. Continuous improvement

3.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

3.2 The Supplier should present new ways of working to the Buyer during monthly Service re-view meetings. These can move to quarterly if DVSA are happy with the successful supplier’s performance.

3.3 Changes to the way in which the Services are to be delivered must be brought to the Buyer’s attention and agreed prior to any changes being implemented.

3.4 It is expected that overarching KPIs will be reported against and monitored monthly.

3.5 The Supplier will provide the DVSA with performance monitoring reports which will provide the following information, as a minimum, in relation to the service period just ended:

• for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period

• a summary of all failures to achieve Service Levels that occurred during that Service Period

• details of any Critical Service Level Failures

• for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence

3.6 Monthly performance review meetings will be held to discuss the performance monitoring reports, what has been completed, lessons learned, actions outstanding, business and requirements for the forthcoming period. The monthly meeting will take place one (1) week following the performance monitoring report being sent to the DVSA. The meetings will be at-tended by DVSA and Supplier representative(s) and full minutes taken for audit purposes.

## 4. Quality

## The Potential Provider shall comply with all the relevant legislation, organisational and cross government policy and guidelines in relation to data and asset security including but not limited to: Data Protection Act 2018, General Data Protection Regulation (UK GDPR 2018), HMG Security Policy Framework, Cabinet Office Minimum Cyber Security Standard (2018), National Cyber Security Centre Cloud Security Principles.

## The Potential Provider shall be Cyber Essentials or Cyber Essentials Plus certified preferably ISO 27001:2013 Information Security Management Standards certified.

**Joint Schedule 1 (Definitions)**

* 1. In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.
  2. If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.
  3. In each Contract, unless the context otherwise requires:
     1. the singular includes the plural and vice versa;
     2. reference to a gender includes the other gender and the neuter;
     3. references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Central Government Body;
     4. a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;
     5. the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";
     6. references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;
     7. references to "**representations**" shall be construed as references to present facts, to "**warranties**" as references to present and future facts and to "**undertakings"** as references to obligations under the Contract;
     8. references to **"Clauses"** and **"Schedules"** are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;
     9. references to **"Paragraphs"** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;
     10. references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;
     11. the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract;
     12. where the Buyer is a Central Government Body it shall be treated as contracting with the Crown as a whole;
     13. any reference in a Contract which immediately before Exit Day was a reference to (as it has effect from time to time):
         1. any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement (“**EU References**”) which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 shall be read on and after Exit Day as a reference to the EU References as they form part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and
         2. any EU institution or EU authority or other such EU body shall be read on and after Exit Day as a reference to the UK institution, authority or body to which its functions were transferred; and
     14. unless otherwise provided, references to “**Buyer**” shall be construed as including Exempt Buyers; and
     15. unless otherwise provided, references to “**Call-Off Contract**” and “**Contract**” shall be construed as including Exempt Call-off Contracts.
  4. In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

|  |  |
| --- | --- |
| **"Achieve"** | in respect of a Test, to successfully pass such Test without any Test Issues and in respect of a Milestone, the issue of a Satisfaction Certificate in respect of that Milestone and "**Achieved**", "**Achieving**" and "**Achievement**" shall be construed accordingly; |
| **"Additional Insurances"** | insurance requirements relating to a Call-Off Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements); |
| **"Admin Fee”** | means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees; |
| **"Affected Party"** | the Party seeking to claim relief in respect of a Force Majeure Event; |
| **"Affiliates"** | in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time; |
| **“Annex”** | extra information which supports a Schedule; |
| **"Approval"** | the prior written consent of the Buyer and "**Approve**" and "**Approved**" shall be construed accordingly; |
| **"Audit"** | the Relevant Authority’s right to:   1. verify the accuracy of the Charges and any other amounts payable by a Buyer under a Call-Off Contract (including proposed or actual variations to them in accordance with the Contract); 2. verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services; 3. verify the Open Book Data; 4. verify the Supplier’s and each Subcontractor’s compliance with the Contract and applicable Law; 5. identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations; 6. identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables; 7. obtain such information as is necessary to fulfil the Relevant Authority’s obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; 8. review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract; 9. carry out the Relevant Authority’s internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts; 10. enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant Authority has used its resources; or 11. verify the accuracy and completeness of any Management Information delivered or required by the Framework Contract; |
| **"Auditor"** | 1. the Relevant Authority’s internal and external auditors; 2. the Relevant Authority’s statutory or regulatory auditors; 3. the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; 4. HM Treasury or the Cabinet Office; 5. any party formally appointed by the Relevant Authority to carry out audit or similar review functions; and 6. successors or assigns of any of the above; |
| **"Authority"** | CCS and each Buyer; |
| **"Authority Cause"** | any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier; |
| **"BACS"** | the Bankers’ Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom; |
| **"Beneficiary"** | a Party having (or claiming to have) the benefit of an indemnity under this Contract; |
| **"Buyer"** | the relevant public sector purchaser identified as such in the Order Form; |
| **"Buyer Assets"** | the Buyer’s infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract; |
| **"Buyer Authorised Representative"** | the representative appointed by the Buyer from time to time in relation to the Call-Off Contract initially identified in the Order Form; |
| **"Buyer Premises"** | premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them); |
| **"Call-Off Contract"** | the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the Framework Contract), which consists of the terms set out and referred to in the Order Form; |
| **"Call-Off Contract Period"** | the Contract Period in respect of the Call-Off Contract; |
| **"Call-Off Expiry Date"** | the scheduled date of the end of a Call-Off Contract as stated in the Order Form; |
| **"Call-Off Incorporated Terms"** | the contractual terms applicable to the Call-Off Contract specified under the relevant heading in the Order Form; |
| **"Call-Off Initial Period"** | the Initial Period of a Call-Off Contract specified in the Order Form; |
| **"Call-Off Optional Extension Period"** | such period or periods beyond which the Call-Off Initial Period may be extended as specified in the Order Form; |
| **"Call-Off Procedure"** | the process for awarding a Call-Off Contract pursuant to Clause 2 (How the contract works) and Framework Schedule 7 (Call-Off Award Procedure); |
| **"Call-Off Special Terms"** | any additional terms and conditions specified in the Order Form incorporated into the applicable Call-Off Contract; |
| **"Call-Off Start Date"** | the date of start of a Call-Off Contract as stated in the Order Form; |
| **"Call-Off Tender"** | the tender submitted by the Supplier in response to the Buyer’s Statement of Requirements following a Further Competition Procedure and set out at Call-Off Schedule 4 (Call-Off Tender); |
| **"CCS"** | the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP; |
| **"CCS Authorised Representative"** | the representative appointed by CCS from time to time in relation to the Framework Contract initially identified in the Framework Award Form; |
| **"Central Government Body"** | a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:   * 1. Government Department;   2. Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);   3. Non-Ministerial Department; or   4. Executive Agency; |
| **"Change in Law"** | any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date; |
| **"Change of Control"** | a change of control within the meaning of Section 450 of the Corporation Tax Act 2010; |
| **"Charges"** | the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Call-Off Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Call-Off Contract less any Deductions; |
| **"Claim"** | any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract; |
| **"Commercially Sensitive Information"** | the Confidential Information listed in the Framework Award Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss; |
| **"Comparable Supply"** | the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables; |
| **"Compliance Officer"** | the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations; |
| **"Confidential Information"** | means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as **"confidential"**) or which ought reasonably to be considered to be confidential; |
| **"Conflict of Interest"** | a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS; |
| **"Contract"** | either the Framework Contract or the Call-Off Contract, as the context requires; |
| **"Contract Period"** | the term of either a Framework Contract or Call-Off Contract on and from the earlier of the:  a) applicable Start Date; or  b) the Effective Date  up to and including the applicable End Date; |
| **"Contract Value"** | the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier; |
| **"Contract Year"** | a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof; |
| **"Control"** | control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "**Controlled**" shall be construed accordingly; |
| **“Controller”** | has the meaning given to it in the UK GDPR; |
| **“Core Terms”** | CCS’ terms and conditions for common goods and services which govern how Suppliers must interact with CCS and Buyers under Framework Contracts and Call-Off Contracts; |
| **"Costs"** | the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables:   * 1. the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Work Day, of engaging the Supplier Staff, including:      1. base salary paid to the Supplier Staff;      2. employer’s National Insurance contributions;      3. pension contributions;      4. car allowances;      5. any other contractual employment benefits;      6. staff training;      7. work place accommodation;      8. work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and      9. reasonable recruitment costs, as agreed with the Buyer;   2. costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets;   3. operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables; and   4. Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables;   but excluding:   * 1. Overhead;   2. financing or similar costs;   3. maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Call-Off Contract Period whether in relation to Supplier Assets or otherwise;   4. taxation;   5. fines and penalties;   6. amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and   7. non-cash items (including depreciation, amortisation, impairments and movements in provisions). |
| **"CRTPA"** | the Contract Rights of Third Parties Act 1999; |
| **“"Cyber Essentials Equivalent"** | ISO27001 certification where:   1. the Cyber Essentials requirements, at either basic or Plus levels as appropriate, have been included in the scope, and verified as such; and 2. the certification body carrying out this verification is approved to issue a Cyber Essentials certificate by one of the accreditation bodies   This would be regarded as holding an equivalent standard to Cyber Essentials. |
| **“Data Protection Impact Assessment”** | an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data; |
| **"Data Protection Legislation"** | (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 Protection Liability Cap”** | the amount specified in the Framework Award Form; |
| **"Data Protection Officer"** | has the meaning given to it in the UK GDPR; |
| **"Data Subject"** | has the meaning given to it in the UK GDPR; |
| **"Data Subject Access Request"** | a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data; |
| **"Deductions"** | all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under a Call-Off Contract; |
| **"Default"** | any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority; |
| **"Default Management Charge"** | has the meaning given to it in Paragraph 8.1.1 of Framework Schedule 5 (Management Charges and Information); |
| **"Delay Payments"** | the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan; |
| **"Deliverables"** | Goods and/or Services that may be ordered under the Contract including the Documentation; |
| **"Delivery"** | delivery of the relevant Deliverable or Milestone in accordance with the terms of a Call-Off Contract as confirmed and accepted by the Buyer by either (a) confirmation in writing to the Supplier; or (b) where Call-Off Schedule 13 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. "**Deliver**" and "**Delivered**" shall be construed accordingly; |
| **"Disclosing Party"** | the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential); |
| **"Dispute"** | any claim, dispute or difference (whether contractual or non-contractual) arising out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts; |
| **"Dispute Resolution Procedure"** | the dispute resolution procedure set out in Clause 34 (Resolving disputes); |
| **"Documentation"** | descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as:   * 1. would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables   2. is required by the Supplier in order to provide the Deliverables; and/or   3. has been or shall be generated for the purpose of providing the Deliverables; |
| **"DOTAS"** | the Disclosure of Tax Avoidance Schemes rules which require a promoter of Tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions; |
| **“DPA 2018”** | the Data Protection Act 2018; |
| **"Due Diligence Information"** | any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date; |
| **“Effective Date”** | the date on which the final Party has signed the Contract; |
| **"EIR"** | the Environmental Information Regulations 2004; |
| **“Electronic Invoice”** | an invoice which has been issued, transmitted and received in a structured electronic format which allows for its automatic and electronic processing and which complies with (a) the European standard and (b) any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870; |
| **"Employment Regulations"** | the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC; |
| **"End Date"** | the earlier of:   * 1. the Expiry Date (as extended by any Extension Period exercised by the Relevant Authority under Clause 10.1.2); or   2. if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract; |
| **"Environmental Policy"** | to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer; |
| **"Equality and Human Rights Commission"** | the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time; |
| **“Estimated Year 1 Charges”** | the anticipated total Charges payable by the Buyer in the first Contract Year specified in the Order Form; |

|  |  |
| --- | --- |
| **"Estimated Yearly Charges"** | means for the purposes of calculating each Party’s annual liability under clause 11.2 :  i)  in the first Contract Year, the Estimated Year 1 Charges; or  ii) in the any subsequent Contract Years, the Charges paid or payable in the previous Call-off Contract Year; or      iii) after the end of the Call-off Contract, the Charges paid or payable in the last Contract Year during the Call-off Contract Period; |
| “**Exempt Buyer**” | a public sector purchaser that is:   1. eligible to use the Framework Contract; and 2. is entering into an Exempt Call-off Contract that is not subject to (as applicable) any of:    1. the Regulations;    2. the Concession Contracts Regulations 2016 (SI 2016/273);    3. the Utilities Contracts Regulations 2016 (SI 2016/274);    4. the Defence and Security Public Contracts Regulations 2011 (SI 2011/1848);    5. the Remedies Directive (2007/66/EC);    6. Directive 2014/23/EU of the European Parliament and Council;    7. Directive 2014/24/EU of the European Parliament and Council;    8. Directive 2014/25/EU of the European Parliament and Council; or    9. Directive 2009/81/EC of the European Parliament and Council; |
| “**Exempt Call-off Contract**” | the contract between the Exempt Buyer and the Supplier for Deliverables which consists of the terms set out and referred to in the Order Form incorporating and, where necessary, amending, refining or adding to the terms of the Framework Contract; |
| “**Exempt Procurement Amendments**” | any amendments, refinements or additions to any of the terms of the Framework Contract made through the Exempt Call-off Contract to reflect the specific needs of an Exempt Buyer to the extent permitted by and in accordance with any legal requirements applicable to that Exempt Buyer; |

|  |  |
| --- | --- |
| **"Existing IPR"** | any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise); |
| **“Exit Day”** | shall have the meaning in the European Union (Withdrawal) Act 2018; |
| **"Expiry Date"** | the Framework Expiry Date or the Call-Off Expiry Date (as the context dictates); |
| **"Extension Period"** | the Framework Optional Extension Period or the Call-Off Optional Extension Period as the context dictates; |
| **“Financial Reports”** | a report by the Supplier to the Buyer that:  a) provides a true and fair reflection of the Costs and Supplier Profit Margin forecast by the Supplier;  b) provides a true and fair reflection of the costs and expenses to be incurred by Key Subcontractors (as requested by the Buyer);  c) is in the same software package (Microsoft Excel or Microsoft Word), layout and format as the blank templates which have been issued by the Buyer to the Supplier on or before the Start Date for the purposes of the Contract; and  is certified by the Supplier’s Chief Financial Officer or Director of Finance; |
| **"FOIA"** | the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation; |
| **"Force Majeure Event"** | any event outside the reasonable control of either Party affecting its performance of its obligations under the Contract arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including:   * 1. riots, civil commotion, war or armed conflict;   2. acts of terrorism;   3. acts of government, local government or regulatory bodies;   4. fire, flood, storm or earthquake or other natural disaster,   but excluding any industrial dispute relating to the Supplier, the Supplier Staff or any other failure in the Supplier or the Subcontractor's supply chain; |
| **"Force Majeure Notice"** | a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event; |
| **"Framework Award Form"** | the document outlining the Framework Incorporated Terms and crucial information required for the Framework Contract, to be executed by the Supplier and CCS; |
| **"Framework Contract"** | the framework agreement established between CCS and the Supplier in accordance with Regulation 33 by the Framework Award Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the notice published on the Find a Tender Service; |
| **"Framework Contract Period"** | the period from the Framework Start Date until the End Date of the Framework Contract; |
| **"Framework Expiry Date"** | the scheduled date of the end of the Framework Contract as stated in the Framework Award Form; |
| **"Framework Incorporated Terms"** | the contractual terms applicable to the Framework Contract specified in the Framework Award Form; |
| **"Framework Optional Extension Period"** | such period or periods beyond which the Framework Contract Period may be extended as specified in the Framework Award Form; |
| **"Framework Price(s)"** | the price(s) applicable to the provision of the Deliverables set out in Framework Schedule 3 (Framework Prices); |
| **"Framework Special Terms"** | any additional terms and conditions specified in the Framework Award Form incorporated into the Framework Contract; |
| **"Framework Start Date"** | the date of start of the Framework Contract as stated in the Framework Award Form; |
| **"Framework Tender Response"** | the tender submitted by the Supplier to CCS and annexed to or referred to in Framework Schedule 2 (Framework Tender); |
| **"Further Competition Procedure"** | the further competition procedure described in Framework Schedule 7 (Call-Off Award Procedure); |
| **"UK GDPR"** | the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679); |
| **"General Anti-Abuse Rule"** | * 1. the legislation in Part 5 of the Finance Act 2013 and; and   2. any future legislation introduced into parliament to counteract Tax advantages arising from abusive arrangements to avoid National Insurance contributions; |
| **"General Change in Law"** | a Change in Law where the change is of a general legislative nature (including Tax or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply; |
| **“Gold Contract”** | a Call-Off Contract categorised as a Gold contract using the Cabinet Office Contract Tiering Tool; |
| **"Goods"** | goods made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form ; |
| **"Good Industry Practice"** | standards, practices, methods and procedures conforming to the Law and the exercise of the 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 within the relevant industry or business sector; |
| **"Government"** | the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf; |
| **"Government Data"** | the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority’s Confidential Information, and which:   * + 1. are supplied to the Supplier by or on behalf of the Authority; or     2. the Supplier is required to generate, process, store or transmit pursuant to a Contract; |
| **"Guarantor"** | the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract; |
| **"Halifax Abuse Principle"** | the principle explained in the CJEU Case C-255/02 Halifax and others; |
| **“HM Government”** | Her Majesty's Government; |
| **"HMRC"** | Her Majesty’s Revenue and Customs; |
| **"ICT Policy"** | the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure; |
| **"Impact Assessment"** | an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:   * 1. details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract;   2. details of the cost of implementing the proposed Variation;   3. details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Framework Prices/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;   4. a timetable for the implementation, together with any proposals for the testing of the Variation; and   5. such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request; |
| **"Implementation Plan"** | the plan for provision of the Deliverables set out in Call-Off Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer; |
| **"Indemnifier"** | a Party from whom an indemnity is sought under this Contract; |
| **“Independent Control”** | where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and “**Independent Controller**” shall be construed accordingly; |
| **"Indexation"** | the adjustment of an amount or sum in accordance with Framework Schedule 3 (Framework Prices) and the relevant Order Form; |
| **"Information"** | has the meaning given under section 84 of the Freedom of Information Act 2000; |
| **"Information Commissioner"** | the UK’s independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies; |
| **"Initial Period"** | the initial term of a Contract specified in the Framework Award Form or the Order Form, as the context requires; |
| **"Insolvency Event"** | with respect to any person, means:  (a) that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or:  (i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or  (ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986;  (b) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;  (c) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person;  (d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person’s assets and such attachment or process is not discharged within 14 days;  (e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;  (f) where that person is a company, a LLP or a partnership:  (i) a petition is presented (which is not dismissed within 14 days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;  (ii) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at Court or given or if an administrator is appointed, over that person;  (iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or  (iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or  (g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above; |
| **"Installation Works"** | all works which the Supplier is to carry out at the beginning of the Call-Off Contract Period to install the Goods in accordance with the Call-Off Contract; |
| **"Intellectual Property Rights" or "IPR"** | * 1. 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 or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information;   2. 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; and   3. all other rights having equivalent or similar effect in any country or jurisdiction; |
| **"Invoicing Address"** | the address to which the Supplier shall invoice the Buyer as specified in the Order Form; |
| **"IPR Claim"** | any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract; |
| **"IR35"** | the off-payroll rules requiring individuals who work through their company pay the same income tax and National Insurance contributions as an employee which can be found online at: <https://www.gov.uk/guidance/ir35-find-out-if-it-applies>; |
| **“ISO”** | International Organization for Standardization; |
| **“Joint Controller Agreement”** | the agreement (if any) entered into between the Relevant Authority and the Supplier substantially in the form set out in Annex 2 of Joint Schedule 11 (*Processing Data*); |
| **“Joint Controllers”** | where two or more Controllers jointly determine the purposes and means of Processing; |
| **"Key Staff"** | the individuals (if any) identified as such in the Order Form; |
| **"Key Sub-Contract"** | each Sub-Contract with a Key Subcontractor; |
| **"Key Subcontractor"** | any Subcontractor:   * 1. which is relied upon to deliver any work package within the Deliverables in their entirety; and/or   2. which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or   3. with a Sub-Contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under the Call-Off Contract,   and the Supplier shall list all such Key Subcontractors in section 19 of the Framework Award Form and in the Key Subcontractor Section in Order Form; |
| **"Know-How"** | all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party’s possession before the applicable Start Date; |
| **"Law"** | any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply; |
| **"Losses"** | 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 "**Loss**" shall be interpreted accordingly; |
| **"Lots"** | the number of lots specified in Framework Schedule 1 (Specification), if applicable; |
| **"Management Charge"** | the sum specified in the Framework Award Form payable by the Supplier to CCS in accordance with Framework Schedule 5 (Management Charges and Information); |
| **"Management Information" or “MI”** | the management information specified in Framework Schedule 5 (Management Charges and Information); |
| **“MI Default”** | means whentwo (2) MI Reports are not provided in any rolling six (6) month period |
| **"MI Failure"** | means when an MI report:   * 1. contains any material errors or material omissions or a missing mandatory field; or   2. is submitted using an incorrect MI reporting Template; or   3. is not submitted by the reporting date (including where a declaration of no business should have been filed); |
| **"MI Report"** | means a report containing Management Information submitted to the Authority in accordance with Framework Schedule 5 (Management Charges and Information); |
| **"MI Reporting Template"** | means the form of report set out in the Annex to Framework Schedule 5 (Management Charges and Information) setting out the information the Supplier is required to supply to the Authority; |
| **"Milestone"** | an event or task described in the Implementation Plan; |
| **"Milestone Date"** | the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved; |
| **"Month"** | a calendar month and "**Monthly**" shall be interpreted accordingly; |
| **"National Insurance"** | contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004); |
| **"New IPR"** | * 1. IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or   2. IPR in or arising as a result of the performance of the Supplier’s obligations under a Contract and all updates and amendments to the same;   but shall not include the Supplier’s Existing IPR; |
| **"Occasion of Tax Non–Compliance"** | where:   * 1. any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of:      1. a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any Tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;      2. the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or   2. any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for Tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion; |
| **"Open Book Data "** | complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Call-Off Contract, including details and all assumptions relating to:   * 1. the Supplier’s Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables;   2. operating expenditure relating to the provision of the Deliverables including an analysis showing:      1. the unit costs and quantity of Goods and any other consumables and bought-in Deliverables;      2. staff costs broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each grade;      3. a list of Costs underpinning those rates for each grade, being the agreed rate less the Supplier Profit Margin; and      4. Reimbursable Expenses, if allowed under the Order Form;   3. Overheads;   4. all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables;   5. the Supplier Profit achieved over the Framework Contract Period and on an annual basis;   6. confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier;   7. an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and   8. the actual Costs profile for each Service Period; |
| **"Order"** | means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract; |
| **"Order Form"** | a completed Order Form Template (or equivalent information issued by the Buyer) used to create a Call-Off Contract; |
| **"Order Form Template"** | the template in Framework Schedule 6 (Order Form Template and Call-Off Schedules); |
| **"Other Contracting Authority"** | any actual or potential Buyer under the Framework Contract; |
| **"Overhead"** | those amounts which are intended to recover a proportion of the Supplier’s or the Key Subcontractor’s (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs"; |
| **"Parliament"** | takes its natural meaning as interpreted by Law; |
| **"Party"** | in the context of the Framework Contract, CCS or the Supplier, and in the in the context of a Call-Off Contract the Buyer or the Supplier. "**Parties**" shall mean both of them where the context permits; |
| **"Performance Indicators" or "PIs"** | the performance measurements and targets in respect of the Supplier’s performance of the Framework Contract set out in Framework Schedule 4 (Framework Management); |
| **"Personal Data"** | has the meaning given to it in the UK GDPR; |
| **“Personal Data Breach”** | has the meaning given to it in the UK GDPR; |
| **“Personnel”** | all directors, officers, employees, agents, consultants and suppliers of a Party and/or of any Subcontractor and/or Subprocessor engaged in the performance of its obligations under a Contract; |
| **"Prescribed Person"** | a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in ‘Whistleblowing: list of prescribed people and bodies’, 24 November 2016, available online at: <https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies>; |
| **“Processing”** | has the meaning given to it in the UK GDPR; |
| **“Processor”** | has the meaning given to it in the UK GDPR; |
| **"Progress Meeting"** | a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative; |
| **"Progress Meeting Frequency"** | the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form; |
| **“Progress Report”** | a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates; |
| **“Progress Report Frequency”** | the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form; |
| **“Prohibited Acts”** | * 1. to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to:      1. induce that person to perform improperly a relevant function or activity; or      2. reward that person for improper performance of a relevant function or activity;   2. to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with each Contract; or   3. committing any offence:      1. under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or      2. under legislation or common law concerning fraudulent acts; or      3. defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or   4. any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK; |
| **“Protective Measures”** | appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Framework Schedule 9 (Cyber Essentials Scheme), if applicable, in the case of the Framework Contract or Call-Off Schedule 9 (Security), if applicable, in the case of a Call-Off Contract. |
| **“Rating Agency”** | as defined in the Framework Award Form or the Order Form, as the context requires; |
| **“Recall”** | a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance; |
| **"Recipient Party"** | the Party which receives or obtains directly or indirectly Confidential Information; |
| **"Rectification Plan"** | the Supplier’s plan (or revised plan) to rectify it’s breach using the template in Joint Schedule 10 (Rectification Plan) which shall include:   * 1. full details of the Default that has occurred, including a root cause analysis;   2. the actual or anticipated effect of the Default; and   3. the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable); |
| **"Rectification Plan Process"** | the process set out in Clause 10.3.1 to 10.3.4 (Rectification Plan Process); |
| **"Regulations"** | the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires); |
| **"Reimbursable Expenses"** | the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Buyer's expenses policy current from time to time, but not including:   * 1. travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and   2. subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed; |
| **"Relevant Authority"** | the Authority which is party to the Contract to which a right or obligation is owed, as the context requires; |
| **"Relevant Authority's Confidential Information"** | * 1. all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR);   2. any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority’s attention or into the Relevant Authority’s possession in connection with a Contract; and   information derived from any of the above; |
| **"Relevant Requirements"** | all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010; |
| **"Relevant Tax Authority"** | HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established; |
| **"Reminder Notice"** | a notice sent in accordance with Clause 10.5 given by the Supplier to the Buyer providing notification that payment has not been received on time; |
| **"Replacement Deliverables"** | any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Call-Off Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party; |
| **"Replacement Subcontractor"** | a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor); |
| **"Replacement Supplier"** | any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer; |
| **"Request For Information"** | a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs; |
| **"Required Insurances"** | the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form; |
| **“RTI”** | Real Time Information; |
| **"Satisfaction Certificate"** | the certificate (materially in the form of the document contained in of Part B of Call-Off Schedule 13 (Implementation Plan and Testing) or as agreed by the Parties where Call-Off Schedule 13 is not used in this Contract) granted by the Buyer when the Supplier has met all of the requirements of an Order, Achieved a Milestone or a Test; |
| **"Security Management Plan"** | the Supplier's security management plan prepared pursuant to Call-Off Schedule 9 (Security) (if applicable); |
| **"Security Policy"** | the Buyer's security policy, referred to in the Order Form, in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier; |
| **"Self Audit Certificate"** | means the certificate in the form as set out in Framework Schedule 8 (Self Audit Certificate); |
| **"Serious Fraud Office"** | the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time; |
| **“Service Levels”** | any service levels applicable to the provision of the Deliverables under the Call Off Contract (which, where Call Off Schedule 14 (Service Levels) is used in this Contract, are specified in the Annex to Part A of such Schedule); |
| **"Service Period"** | has the meaning given to it in the Order Form; |
| **"Services"** | services made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form; |
| **"Service Transfer"** | any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor; |
| **"Service Transfer Date"** | the date of a Service Transfer; |
| **"Sites"** | any premises (including the Buyer Premises, the Supplier’s premises or third party premises) from, to or at which:   * 1. the Deliverables are (or are to be) provided; or   2. the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; |
| **"SME"** | an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium enterprises; |
| **"Special Terms"** | any additional Clauses set out in the Framework Award Form or Order Form which shall form part of the respective Contract; |
| **"Specific Change in Law"** | a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date; |
| **"Specification"** | the specification set out in Framework Schedule 1 (Specification), as may, in relation to a Call-Off Contract, be supplemented by the Order Form; |
| **"Standards"** | any:   * 1. standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with;   2. standards detailed in the specification in Schedule 1 (Specification);   3. standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time;   4. relevant Government codes of practice and guidance applicable from time to time; |
| **"Start Date"** | in the case of the Framework Contract, the date specified on the Framework Award Form, and in the case of a Call-Off Contract, the date specified in the Order Form; |
| **"Statement of Requirements"** | a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Call-Off Procedure; |
| **"Storage Media"** | the part of any device that is capable of storing and retrieving data; |
| **"Sub-Contract"** | any contract or agreement (or proposed contract or agreement), other than a Call-Off Contract or the Framework Contract, pursuant to which a third party:   * 1. provides the Deliverables (or any part of them);   2. provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or   3. is responsible for the management, direction or control of the provision of the Deliverables (or any part of them); |
| **"Subcontractor"** | any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person; |
| **"Subprocessor"** | any third Party appointed to process Personal Data on behalf of that Processor related to a Contract; |
| **"Supplier"** | the person, firm or company identified in the Framework Award Form; |
| **"Supplier Assets"** | all assets and rights used by the Supplier to provide the Deliverables in accordance with the Call-Off Contract but excluding the Buyer Assets; |
| **"Supplier Authorised Representative"** | the representative appointed by the Supplier named in the Framework Award Form, or later defined in a Call-Off Contract; |
| **"Supplier's Confidential Information"** | * 1. any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier;   2. any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier’s attention or into the Supplier’s possession in connection with a Contract;   3. Information derived from any of (a) and (b) above; |
| **"Supplier's Contract Manager** | the person identified in the Order Form appointed by the Supplier to oversee the operation of the Call-Off Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment; |
| **"Supplier Equipment"** | the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Call-Off Contract; |
| **"Supplier Marketing Contact"** | shall be the person identified in the Framework Award Form; |
| **"Supplier Non-Performance"** | where the Supplier has failed to:   * 1. Achieve a Milestone by its Milestone Date;   2. provide the Goods and/or Services in accordance with the Service Levels ; and/or   3. comply with an obligation under a Contract; |
| **"Supplier Profit"** | in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions) and total Costs (in nominal cash flow terms) in respect of a Call-Off Contract for the relevant period; |
| **"Supplier Profit Margin"** | in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage; |
| **"Supplier Staff"** | all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier’s obligations under a Contract; |
| **"Supporting Documentation"** | sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Call-Off Contract detailed in the information are properly payable; |
| **“Tax”** | 1. all forms of taxation whether direct or indirect; 2. national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction; 3. all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions. levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and 4. any penalty, fine, surcharge, interest, charges or costs relating to any of the above,   in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction; |
| **"Termination Notice"** | a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate a Contract on a specified date and setting out the grounds for termination; |
| **"Test Issue"** | any variance or non-conformity of the Deliverables from their requirements as set out in a Call-Off Contract; |
| **"Test Plan"** | a plan:   * 1. for the Testing of the Deliverables; and   2. setting out other agreed criteria related to the achievement of Milestones; |
| **"Tests "** | any tests required to be carried out pursuant to a Call-Off Contract as set out in the Test Plan or elsewhere in a Call-Off Contract and "**Tested**" and “**Testing**” shall be construed accordingly; |
| **"Third Party IPR"** | Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables; |
| **"Transferring Supplier Employees"** | those employees of the Supplier and/or the Supplier’s Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date; |
| **"Transparency Information"** | the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for –  (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and  (ii) Commercially Sensitive Information; |
| **"Transparency Reports"** | the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Call-Off Schedule 1 (Transparency Reports); |
| **“TUPE”** | Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other regulations or UK legislation implementing the Acquired Rights Directive |
| **“United Kingdom”** | the country that consists of England, Scotland, Wales, and Northern Ireland |
| **"Variation"** | any change to a Contract; |
| **"Variation Form"** | the form set out in Joint Schedule 2 (Variation Form); |
| **"Variation Procedure"** | the procedure set out in Clause 24 (Changing the contract); |
| **"VAT"** | value added tax in accordance with the provisions of the Value Added Tax Act 1994; |
| **"VCSE"** | a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives; |
| **"Worker"** | any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables; |
| **"Working Day"** | any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form; |
| **"Work Day"** | Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day; and |
| **"Work Hours"** | the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks. |

**Joint Schedule 2 (Variation Form)**

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

|  |  |  |
| --- | --- | --- |
| **Contract Details** | | |
| This variation is between: | **[delete** as applicable:CCS / Buyer**]** ("**CCS” “the Buyer"**)  And  **[insert** name of Supplier**]** (**"the Supplier"**) | |
| Contract name: | **[insert** name of contract to be changed] **(“the Contract”)** | |
| Contract reference number: | **[insert** contract reference number] | |
| **Details of Proposed Variation** | | |
| Variation initiated by: | **[delete** as applicable: CCS/Buyer/Supplier] | |
| Variation number: | **[insert** variation number] | |
| Date variation is raised: | **[insert** date] | |
| Proposed variation |  | |
| Reason for the variation: | **[insert** reason] | |
| An Impact Assessment shall be provided within: | **[insert** number] days | |
| **Impact of Variation** | | |
| Likely impact of the proposed variation: | **[Supplier to insert** assessment of impact] | |
| **Outcome of Variation** | | |
| Contract variation: | This Contract detailed above is varied as follows:   * **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause] | |
| Financial variation: | Original Contract Value: | £ **[insert** amount] |
| Additional cost due to variation: | £ **[insert** amount] |
| New Contract value: | £ **[insert** amount] |

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete** as applicable:CCS / Buyer**]**
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the **[delete** as applicable:CCS / Buyer**]**

|  |  |
| --- | --- |
| Signature |  |
| Date |  |
| Name (in Capitals) |  |
| Address |  |
|  |  |

Signed by an authorised signatory to sign for and on behalf of the Supplier

|  |  |
| --- | --- |
| Signature |  |
| Date |  |
| Name (in Capitals) |  |
| Address |  |

**Joint Schedule 3 (Insurance Requirements)**

1. **The insurance you need to have**

## The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("Additional Insurances") and any other insurances as may be required by applicable Law (together the “Insurances”). The Supplier shall ensure that each of the Insurances is effective no later than:

* + 1. the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
    2. the Call-Off Contract Effective Date in respect of the Additional Insurances.

## The Insurances shall be:

* + 1. maintained in accordance with Good Industry Practice;
    2. (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;
    3. taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
    4. maintained for at least six (6) years after the End Date.
  1. The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

1. **How to manage the insurance**
   1. Without limiting the other provisions of this Contract, the Supplier shall:
      1. take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;
      2. promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
      3. hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.
2. **What happens if you aren’t insured**
   1. The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.
   2. Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.
3. **Evidence of insurance you must provide**
   1. The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.
4. **Making sure you are insured to the required amount**
   1. The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.
5. **Cancelled Insurance**
   1. The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
   2. The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.
6. **Insurance claims**
   1. The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.
   2. Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.
   3. Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
   4. Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

**ANNEX: REQUIRED INSURANCES**

The Supplier shall hold the following [standard] insurance cover from the Framework Start Date in accordance with this Schedule:

## 1.1 Professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000) – all Lots.

## 1.2 Public liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000) – all Lots.

## 1.3 Employers’ liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000) – all Lots.

1.4 Product liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000) – all Lots.

**Joint Schedule 4 (Commercially Sensitive Information)**

1. **What is the Commercially Sensitive Information?**
   1. In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
   2. Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
   3. Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

| **No.** | **Date** | **Item(s)** | **Duration of Confidentiality** |
| --- | --- | --- | --- |
|  | 03/02/2025 | We consider any information that relates to or concerns the pricing and/or sourcing of any Goods and/or any Services to be supplied under this agreement to be sensitive. | Phoenix Software Ltd considers that all information will remain commercially sensitive (and therefore exempt from disclosure) for a period of five (5) years from the later of the date of the submission of Phoenix Software’s tender response or the commencement date of the agreement. |

**Joint Schedule 6 (Key Subcontractors)  
  
*Not applicable currently, but before use, this schedule has to be approved by both parties***

1. **Restrictions on certain subcontractors**
   1. The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.
   2. The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.
   3. Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to section 18 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:
      1. the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
      2. the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
      3. the proposed Key Subcontractor employs unfit persons.
   4. The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:
      1. the proposed Key Subcontractor’s name, registered office and company registration number;
      2. the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;
      3. where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm’s-length" terms;
      4. for CCS, the Key Sub-Contract price expressed as a percentage of the total projected Framework Price over the Framework Contract Period;
      5. for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and
      6. (where applicable) Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.
   5. If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:
      1. a copy of the proposed Key Sub-Contract; and
      2. any further information reasonably requested by CCS and/or the Buyer.
   6. The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:
      1. provisions which will enable the Supplier to discharge its obligations under the Contracts;
      2. a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;
      3. a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;
      4. a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;
      5. obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:
         1. the data protection requirements set out in Clause 14 (Data protection);
         2. the FOIA and other access request requirements set out in Clause 16 (When you can share information);
         3. the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;
         4. the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and
         5. the conduct of audits set out in Clause 6 (Record keeping and reporting);
      6. provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the Buyer can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and
      7. a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

**Joint Schedule 7 (Financial Difficulties)**

1. **Definitions**
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| **“Applicable Financial Indicators”** | means the financial indicators from Paragraph 5.1 of this Schedule which are to apply to the Monitored Suppliers as set out in Paragraph 5.2 of this Schedule; |
| **“Board”** | means the Supplier’s board of directors; |
| **“Board Confirmation”** | means written confirmation from the Board in accordance with Paragraph 8 of this Schedule; |
| **“Bronze Contract”** | A Call-Off Contract categorised as a Bronze contract using the Cabinet Office Contract Tiering Tool; |
| **“Cabinet Office Markets and Suppliers Team”** | means the UK Government’s team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function; |
| **“Credit Rating Threshold”** | the minimum credit rating level for each entity in the FDE Group as set out in Annex 1 to this Schedule; |
| **“FDE Group”** | means the Supplier, Key Sub-contractors, the Guarantor and the Monitored Suppliers if appropriate; |
| **“Financial Distress Event”** | Any of the events listed in Paragraph 3.1 of this Schedule; |
| **“Financial Distress Remediation Plan”** | a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with the Contract in the event that a Financial Distress Event occurs; |
| **“Financial Indicators”** | in respect of the Supplier, Key Sub-contractors and the Guarantor, means each of the financial indicators set out at paragraph 5.1 of this Schedule and in respect of each Monitored Supplier, means those Applicable Financial Indicators; |
| **“Financial Target Thresholds”** | means the target thresholds for each of the Financial Indicators set out at paragraph 5.1 of this Schedule; |
| **“Monitored Suppliers”** | means those entities specified at paragraph 5.2 of this Schedule; |
| **“Rating Agencies”** | The rating agencies listed in Annex 1 of this Schedule; |
| **“Strategic Supplier”** | means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers. |

1. **Warranties and duty to notify**
   1. The Supplier warrants and represents to the Relevant Authority for the benefit of the Relevant Authority that as at the Effective Date:
      1. the long term credit ratings issued for each entity in the FDE Group by each of the Rating Agencies are as set out in Annex 2 to this Schedule; and
      2. the financial position or, as appropriate, the financial performance of each of the Supplier, Guarantor and Key Sub-contractors satisfies the Financial Target Thresholds.
   2. The Supplier shall promptly notify (or shall procure that its auditors promptly notify) the Relevant Authority in writing if there is any downgrade in the credit rating issued by any Rating Agency for any entity in the FDE Group (and in any event within 5 Working Days of the occurrence of the downgrade).
   3. The Supplier shall:
      1. regularly monitor the credit ratings of each entity in the FDE Group with the Rating Agencies;
      2. monitor and report on the Financial Indicators for each entity in the FDE Group against the Financial Target Thresholds at least at the frequency set out for each at Paragraph 5.1 (where specified) and in any event, on a regular basis and no less than once a year within ninety (90) days after the Accounting Reference Date; and
      3. promptly notify (or shall procure that its auditors promptly notify) the Relevant Authority in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event (and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event).
   4. For the purposes of determining whether a Financial Distress Event has occurred pursuant to the provisions of Paragraphs 3.1, and for the purposes of determining relief under Paragraph 7.1, the credit rating of an FDE Group entity shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated that entity at or below the applicable Credit Rating Threshold.
   5. Each report submitted by the Supplier pursuant to paragraph 2.3.2 shall:
      1. be a single report with separate sections for each of the FDE Group entities;
      2. contain a sufficient level of information to enable the Relevant Authority to verify the calculations that have been made in respect of the Financial Indicators;
      3. include key financial and other supporting information (including any accounts data that has been relied on) as separate annexes;
      4. be based on the audited accounts for the date or period on which the Financial Indicator is based or, where the Financial Indicator is not linked to an accounting period or an accounting reference date, on unaudited management accounts prepared in accordance with their normal timetable; and
      5. include a history of the Financial Indicators reported by the Supplier in graph form to enable the Relevant Authority to easily analyse and assess the trends in financial performance.
2. **Financial Distress events**
   1. The following shall be Financial Distress Events:
      1. the credit rating of an FDE Group entity dropping below the applicable Credit Rating Threshold;
      2. an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;
      3. there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;
      4. an FDE Group entity committing a material breach of covenant to its lenders;
      5. a Key Sub-contractor notifying CCS or the Buyer that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;
      6. any of the following:
         1. commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;
         2. non-payment by an FDE Group entity of any financial indebtedness;
         3. any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;
         4. the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or
         5. the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;

in each case which the Relevant Authority reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance and delivery of the Deliverables in accordance with the Contract; and

* + 1. any [one] of the Financial Indicators set out at Paragraph 5 for any of the FDE Group entities failing to meet the required Financial Target Threshold.

1. **Consequences** of Financial Distress Events
   1. Immediately upon notification by the Supplier of a Financial Distress Event (or if the Relevant Authority becomes aware of a Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and the Relevant Authority shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.
   2. In the event of a late or non-payment of a Key Sub-contractor pursuant to Paragraph 3.1.5, the Relevant Authority shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier 10 Working Days to:
      1. rectify such late or non-payment; or
      2. demonstrate to the Relevant Authority’s reasonable satisfaction that there is a valid reason for late or non-payment.
   3. The Supplier shall (and shall procure that any Monitored Supplier, the Guarantor and/or any relevant Key Sub-contractor shall):
      1. at the request of the Relevant Authority, meet the Relevant Authority as soon as reasonably practicable (and in any event within 3 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Relevant Authority may permit and notify to the Supplier in writing) to review the effect of the Financial Distress Event on the continued performance and delivery of the Services in accordance with the Contract; and
      2. where the Relevant Authority reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1 that the Financial Distress Event could impact on the continued performance and delivery of the Deliverables in accordance with the Contract:
         1. submit to the Relevant Authority for its approval, a draft Financial Distress Remediation Plan as soon as reasonably practicable (and in any event, within 10 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Relevant Authority may permit and notify to the Supplier in writing); and
         2. to the extent that it is legally permitted to do so and subject to Paragraph 4.8, provide such information relating to the Supplier, any Monitored Supplier, Key Sub-contractors and/or the Guarantor as the Buyer may reasonably require in order to understand the risk to the Deliverables, which may include forecasts in relation to cash flow, orders and profits and details of financial measures being considered to mitigate the impact of the Financial Distress Event.
   4. The Relevant Authority shall not withhold its approval of a draft Financial Distress Remediation Plan unreasonably. If the Relevant Authority does not approve the draft Financial Distress Remediation Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Remediation Plan, which shall be resubmitted to the Relevant Authority within 5 Working Days of the rejection of the first draft. This process shall be repeated until the Financial Distress Remediation Plan is approved by the Relevant Authority or referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms under Paragraph 4.5.
   5. If the Relevant Authority considers that the draft Financial Distress Remediation Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not ensure the continued performance of the Supplier’s obligations in accordance with the Contract, then it may either agree a further time period for the development and agreement of the Financial Distress Remediation Plan or escalate any issues with the draft Financial Distress Remediation Plan using the Dispute Resolution Procedure in Clause 34 of the Core Terms.
   6. Following approval of the Financial Distress Remediation Plan by the Relevant Authority, the Supplier shall:
      1. on a regular basis (which shall not be less than fortnightly):
         1. review and make any updates to the Financial Distress Remediation Plan as the Supplier may deem reasonably necessary and/or as may be reasonably requested by the Relevant Authority, so that the plan remains adequate, up to date and ensures the continued performance and delivery of the Deliverables in accordance with this Contract; and
         2. provide a written report to the Relevant Authority setting out its progress against the Financial Distress Remediation Plan, the reasons for any changes made to the Financial Distress Remediation Plan by the Supplier and/or the reasons why the Supplier may have decided not to make any changes;
      2. where updates are made to the Financial Distress Remediation Plan in accordance with Paragraph 4.6.1, submit an updated Financial Distress Remediation Plan to the Relevant Authority for its approval, and the provisions of Paragraphs 4.4 and 4.5 shall apply to the review and approval process for the updated Financial Distress Remediation Plan; and
      3. comply with the Financial Distress Remediation Plan (including any updated Financial Distress Remediation Plan) and ensure that it achieves the financial and performance requirements set out in the Financial Distress Remediation Plan.
   7. Where the Supplier reasonably believes that the relevant Financial Distress Event under Paragraph 4.1 (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Relevant Authority and the Parties may agree that the Supplier shall be relieved of its obligations under Paragraph 4.6.
   8. The Supplier shall use reasonable endeavours to put in place the necessary measures to ensure that the information specified at paragraph 4.3.2(b) is available when required and on request from the Relevant Authority and within reasonable timescales. Such measures may include:
      1. obtaining in advance written authority from Key Sub-contractors, the Guarantor and/or Monitored Suppliers authorising the disclosure of the information to the Buyer and/or entering into confidentiality agreements which permit disclosure;
      2. agreeing in advance with the Relevant Authority, Key Sub-contractors, the Guarantor and/or Monitored Suppliers a form of confidentiality agreement to be entered by the relevant parties to enable the disclosure of the information to the Relevant Authority;
      3. putting in place any other reasonable arrangements to enable the information to be lawfully disclosed to the Relevant Authority (which may include making price sensitive information available to the Relevant Authority’s nominated personnel through confidential arrangements, subject to their consent); and
      4. disclosing the information to the fullest extent that it is lawfully entitled to do so, including through the use of redaction, anonymisation and any other techniques to permit disclosure of the information without breaching a duty of confidentiality.
2. **Financial Indicators**
   1. Subject to the calculation methodology set out at Annex 3 of this Schedule, the Financial Indicators and the corresponding calculations and thresholds used to determine whether a Financial Distress Event has occurred in respect of those Financial Indicators, shall be as follows:

Lots 1 to 7

|  |  |  |  |
| --- | --- | --- | --- |
| **Financial Indicator** | **Calculation1** | **Financial Target Threshold:** | **Monitoring and Reporting Frequency** |
| **1**  **Operating Margin** | *Operating Margin = Operating Profit / Revenue* | *> 8%* | *Tested and reported yearly in arrears within 90 days of each accounting reference date based upon figures for the 12 months ending on the relevant accounting reference date.* |
| **2**  **Net Debt to EBITDA Ratio** | *Net Debt to EBITDA ratio = Net Debt / EBITDA* | *< 3.5 times* | *Tested and reported yearly in arrears within 90 days of each accounting reference date based upon EBITDA for the 12 months ending on, and Net Debt at, the relevant accounting reference date.* |
| **3**  **Net Debt + Net Pension Deficit to EBITDA ratio** | *Net Debt + Net Pension Deficit to EBITDA Ratio = (Net Debt + Net Pension Deficit) / EBITDA* | *< 5 times* | *Tested and reported yearly in arrears within 90 days of each accounting reference date based upon EBITDA for the 12 months ending on, and the Net Debt and Net Pension Deficit at, the relevant accounting reference date* |
| **4**  **Net Interest Paid Cover** | *Net Interest Paid Cover = Earnings Before Interest and Tax / Net Interest Paid* | *> 3 times* | *Tested and reported yearly in arrears within 90 days of each accounting reference date based upon figures for the 12 months ending on the relevant accounting reference date.* |
| **5**  **Acid Ratio** | *Acid Ratio = (Current Assets – Inventories) / Current Liabilities* | *> 0.8 times* | *Tested and reported yearly in arrears within 90 days of each accounting reference date based upon figures at the relevant accounting reference date* |
| **6**  **Net Asset value** | *Net Asset Value = Net Assets* | *> £0* | *Tested and reported yearly in arrears within 90 days of each accounting reference date based upon figures at the relevant accounting reference date* |
| **7**  **Group Exposure Ratio** | *Group Exposure / Gross Assets* | *< 50%* | *Tested and reported yearly in arrears within 90 days of each accounting reference date based upon figures at the relevant accounting reference date* |

Key: 1 – see Annex 3 to this Schedule which sets out the calculation methodology to be used in the calculation of each financial indicator.

* 1. Monitored Suppliers

N/A

|  |  |
| --- | --- |
| **Monitored Supplier** | **Applicable Financial Indicators** |
|  |  |

1. **Termination rights**
   1. The Relevant Authority shall be entitled to terminate the Contract if:
      1. the Supplier fails to notify the Relevant Authority of a Financial Distress Event in accordance with Paragraph 2.3.3;
      2. the Parties fail to agree a Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraphs 4.3 to 4.5; and/or
      3. the Supplier fails to comply with the terms of the Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraph 4.6.3,

which shall be deemed to be an event to which Clause 10.4.1 of the Core Terms applies and Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply accordingly.

1. **Primacy of Credit Ratings**
   1. Without prejudice to the Supplier’s obligations and the Relevant Authority’s rights and remedies under Paragraph 2, if, following the occurrence of a Financial Distress Event pursuant to any of Paragraphs 3.1.2 to 3.1.7, the Rating Agencies review and report subsequently that the credit ratings for the FDE Group entities do not drop below the relevant Credit Rating Thresholds specified for those entities in Annex 2 to this Schedule, then:
      1. the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and
      2. the Relevant Authority shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).
2. **Board confirmation**
   1. If the Contract has been specified as a Critical Service Contract under Paragraph 1.1 of Part B of Annex 1 to Call-Off Schedule 8 (Business Continuity and Disaster Recovery) (if applicable) then, subject to Paragraph 8.4 of this Schedule, the Supplier shall within ninety (90) days after each Accounting Reference Date or within 15 months of the previous Board Confirmation (whichever is the earlier) provide a Board Confirmation to the Relevant Authority in the form set out at Annex 4 to this Schedule, confirming that to the best of the Board’s knowledge and belief, it is not aware of and has no knowledge:
      1. that a Financial Distress Event has occurred since the later of the Effective Date or the previous Board Confirmation or is subsisting; or
      2. of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event.
   2. The Supplier shall ensure that in its preparation of the Board Confirmation it exercises due care and diligence and has made reasonable enquiry of all relevant Supplier Staff and other persons as is reasonably necessary to understand and confirm the position.
   3. In respect of the first Board Confirmation to be provided under this Contract, the Supplier shall provide the Board Confirmation within 15 months of the Effective Date if earlier than the timescale for submission set out in Paragraph 8.1 of this Schedule.
   4. Where the Supplier is unable to provide a Board Confirmation in accordance with Paragraphs 8.1 to 8.3 of this Schedule due to the occurrence of a Financial Distress Event or knowledge of subsisting matters which could reasonably be expected to cause a Financial Distress Event, it will be sufficient for the Supplier to submit in place of the Board Confirmation, a statement from the Board of Directors to the Buyer (and where the Supplier is a Strategic Supplier, the Supplier shall send a copy of the statement to the Cabinet Office Markets and Suppliers Team) setting out full details of any Financial Distress Events that have occurred and/or the matters which could reasonably be expected to cause a Financial Distress Event.
3. **Optional Clauses**
   1. Where a Buyer’s Call-Off Contract is a Bronze Contract, if specified in the Order Form, the terms at Annex 5 shall apply to the Call-Off Contract in place of the foregoing terms of this Joint Schedule 7.

**Annex 1: Rating Agencies and their standard Rating System**

Rating Agency 1 - Dun & Bradstreet

**Annex 2: Credit Ratings and Credit Rating Thresholds**

|  |  |
| --- | --- |
| **Entity** | **Credit rating (long term)** |
| Supplier | 97  Low Risk |
| Guarantor | N/A |
| Key Subcontractor | N/A |
| Monitored Suppliers | N/A |

**Annex 3: Calculation methodology for Financial Indicators**

The Supplier shall ensure that it uses the following general and specific methodologies for calculating the Financial Indicators against the Financial Target Thresholds:

**General methodology**

1. ***Terminology***: The terms referred to in this Annex are those used by UK companies in their financial statements. Where the entity is not a UK company, the corresponding items should be used even if the terminology is slightly different (for example a charity would refer to a surplus or deficit rather than a profit or loss).
2. ***Groups***: Where the entity is the holding company of a group and prepares consolidated financial statements, the consolidated figures should be used.
3. ***Foreign currency conversion***: Figures denominated in foreign currencies should be converted at the exchange rate in force at the relevant date for which the Financial Indicator is being calculated.
4. ***Treatment of non-underlying items***: Financial Indicators should be based on the figures in the financial statements before adjusting for non-underlying items.

**Specific Methodology**

|  |  |
| --- | --- |
| **Financial Indicator** | Specific Methodology |
| **1**  **Operating Margin** | The elements used to calculate the Operating Margin should be shown on the face of the Income Statement in a standard set of financial statements.  Figures for Operating Profit and Revenue should exclude the entity’s share of the results of any joint ventures or Associates.  Where an entity has an operating loss (i.e. where the operating profit is negative), Operating Profit should be taken to be zero. |
| **2**  **Net Debt to EBITDA Ratio** | *“****Net Debt****” = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents*  *“****EBITDA****” = Operating profit + Depreciation charge + Amortisation charge*  The majority of the elements used to calculate the Net Debt to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement and Statement of Cash Flows in a standard set of financial statements but will otherwise be found in the notes to the financial statements.  *Net Debt*: The elements of Net Debt may be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest bearing liabilities (other than retirement benefit obligations) should be included as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but not non-designated hedges). Borrowings should also include balances owed to other group members.  Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing.  Cash and cash equivalents should include short-term financial investments shown in current assets.  Where Net debt is negative (i.e. an entity has net cash), the relevant Financial Target Threshold should be treated as having been met.  *EBITDA*: Operating profit should be shown on the face of the Income Statement and, for the purposes of calculating this Financial Indicator, should include the entity’s share of the results of any joint ventures or Associates. *The depreciation and amortisation charges for the period may be found on the face of the Statement of Cash Flows or in a Note to the Accounts. Where EBITDA is negative, the relevant Financial Target Threshold should be treated as not having been met (unless Net Debt is also negative, in which case the relevant Financial Target Threshold should be treated as having been met).* |
| **3**  **Net Debt + Net Pension Deficit to EBITDA ratio** | *“****Net Debt****” = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents*  *“****Net Pension Deficit****” = Retirement Benefit Obligations – Retirement Benefit Assets*  *“****EBITDA****” = Operating profit + Depreciation charge + Amortisation charge*  The majority of the elements used to calculate the Net Debt + Net Pension Deficit to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement and Statement of Cash Flows in a standard set of financial statements but will otherwise be found in the notes to the financial statements.  *Net Debt*: The elements of Net Debt may be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest bearing liabilities (other than retirement benefit obligations) should be included as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but *not* non-designated hedges). Borrowings should also include balances owed to other group members.  Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing.  Cash and cash equivalents should include short-term financial investments shown in current assets.  *Net Pension Deficit*: Retirement Benefit Obligations and Retirement Benefit Assets may be shown on the face of the Balance Sheet or in the notes to the financial statements. They may also be described as pension benefits / obligations, post-employment obligations or other similar terms.  Where ‘Net Debt + Net Pension Deficit’ is negative, the relevant Financial Target Threshold should be treated as having been met.  *EBITDA*: Operating profit should be shown on the face of the Income Statement and, for the purposes of calculating this Financial Indicator, should include the entity’s share of the results of any joint ventures or Associates.  The depreciation and amortisation charges for the period may be found on the face of the Statement of Cash Flows or in a Note to the Accounts.  Where EBITDA is negative, the relevant Financial Target Threshold should be treated as not having been met (unless ‘Net Debt + Net Pension Deficit’ is also negative, in which case the relevant Financial Target Threshold should be regarded as having been met). |
| **4**  **Net Interest Paid Cover** | *“****Earnings Before Interest and Tax****” = Operating profit*  *“****Net Interest Paid****” = Interest paid – Interest received*  Operating profit should be shown on the face of the Income Statement in a standard set of financial statements and, for the purposes of calculating this Financial Indicator, should include the entity’s share of the results of any joint ventures or Associates.  Interest received and interest paid should be shown on the face of the Cash Flow statement.  Where Net interest paid is negative (i.e. the entity has net interest received), the relevant Financial Target Threshold should be treated as having been met. |
| **5**  **Acid Ratio** | All elements that are used to calculate the Acid Ratio are available on the face of the Balance Sheet in a standard set of financial statements. |
| **6**  **Net Asset value** | Net Assets are shown (but sometimes not labelled) on the face of the Balance Sheet of a standard set of financial statements. Net Assets are sometimes called net worth or ‘Shareholders’ Funds’. They represent the net assets available to the shareholders. Where an entity has a majority interest in another entity in which there are also minority or non-controlling interests (i.e. where it has a subsidiary partially owned by outside investors), Net Assets should be taken inclusive of minority or non-controlling interests (as if the entity owned 100% of such entity). |
| **7**  **Group Exposure Ratio** | *“****Group Exposure****” = Balances owed by Group Undertakings + Contingent liabilities assumed in support of Group Undertakings*  *“****Gross Assets****” = Fixed Assets + Current Assets*  *Group Exposure*: Balances owed by (ie receivable from) Group Undertakings are shown within Fixed assets or Current assets either on the face of the Balance Sheet or in the relevant notes to the financial statements. In many cases there may be no such balances, in particular where an entity is not a member of a group or is itself the ultimate holding company of the group.  Contingent liabilities assumed in support of Group Undertakings are shown in the Contingent Liabilities note in a standard set of financial statements. They include guarantees and security given in support of the borrowings of other group companies, often as part of group borrowing arrangements. Where the contingent liabilities are capped, the capped figure should be taken as their value. Where no cap or maximum is specified, the relevant Financial Target Threshold should automatically be regarded as not having been met.  In many cases an entity may not have assumed any contingent liabilities in support of Group Undertakings, in particular where an entity is not a member of a group or is itself the ultimate holding company of the group.  *Gross Assets*: Both Fixed assets and Current assets are shown on the face of the Balance Sheet. |

**Annex 4: Board Confirmation**

**Supplier Name:**

**Contract Reference Number:**

The Board of Directors acknowledge the requirements set out at paragraph 8 of Joint Schedule 7 (*Financial Distress*) and confirm that the Supplier has exercised due care and diligence and made reasonable enquiry of all relevant Supplier Staff and other persons as is reasonably necessary to enable the Board to prepare this statement.

The Board of Directors confirms, to the best of its knowledge and belief, that as at the date of this Board Confirmation it is not aware of and has no knowledge:

* + - 1. that a Financial Distress Event has occurred since the later of the previous Board Confirmation and the Effective Date or is subsisting; or
      2. of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event

On behalf of the Board of Directors:

Chair …………………………………

Signed …………………………………

Date …………………………………

Director …………………………………

Signed …………………………………

Date …………………………………

**ANNEX 5: OPTIONAL CLAUSES FOR BRONZE CONTRACTS**

1. **Definitions**
   1. In this Annex 5, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

|  |  |
| --- | --- |
| **"Credit Rating Threshold"** | 1. the minimum credit rating level for the Monitored Company as set out in Appendix 2; |
| **"Financial Distress Event"** | 1. the occurrence or one or more of the following events:    1. the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold;    2. the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects;    3. there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party;    4. Monitored Company committing a material breach of covenant to its lenders;    5. a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or    6. any of the following:       1. commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract;       2. non-payment by the Monitored Company of any financial indebtedness;       3. any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or       4. the cancellation or suspension of any financial indebtedness in respect of the Monitored Company 2. in each case which the Relevant Authority reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Call-Off Contract; |
| **"Financial Distress Service Continuity Plan"** | 1. a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with [each Call-Off] Contract in the event that a Financial Distress Event occurs; |
| **“Monitored Company”** | 1. Supplier, the Guarantor or any Key Subcontractor |
| **"Rating Agencies"** | 1. the rating agencies listed in Appendix 1. |

1. **When this Schedule applies**
   1. The Parties shall comply with the provisions of this Annex 5 in relation to the assessment of the financial standing of the Monitored Companies and the consequences of a change to that financial standing.
   2. The terms of this Annex 5 shall survive:
      1. under the Framework Contract until the later of (a) the termination or expiry of the Framework Contract or (b) the latest date of termination or expiry of any call-off contract entered into under the Framework Contract (which might be after the date of termination or expiry of the Framework Contract); and
      2. under the Call-Off Contract until the termination or expiry of the Call-Off Contract.
2. **What happens when your credit rating changes**
   1. The Supplier warrants and represents to the Relevant Authority that as at the Start Date the long term credit ratings issued for the Monitored Companies by each of the Rating Agencies are as set out in Appendix 2.
   2. The Supplier shall promptly (and in any event within five (5) Working Days) notify the Relevant Authority in writing if there is any downgrade in the credit rating issued by any Rating Agency for a Monitored Company.
   3. If there is any downgrade credit rating issued by any Rating Agency for the Monitored Company the Supplier shall ensure that the Monitored Company’s auditors thereafter provide the Relevant Authority within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by the Relevant Authority (such requests not to exceed 4 in any Contract Year) with written calculations of the quick ratio for the Monitored Company as at the end of each Contract Year or such other date as may be requested by the Relevant Authority. For these purposes the "quick ratio" on any date means:



where:

|  |  |
| --- | --- |
| A | is the value at the relevant date of all cash in hand and at the bank of the Monitored Company]; |
| B | is the value of all marketable securities held by the Supplier the Monitored Company determined using closing prices on the Working Day preceding the relevant date; |
| C | is the value at the relevant date of all account receivables of the Monitored]; and |
| D | is the value at the relevant date of the current liabilities of the Monitored Company]. |

* 1. The Supplier shall:
     1. regularly monitor the credit ratings of each Monitored Company with the Rating Agencies; and
     2. promptly notify (or shall procure that its auditors promptly notify) the Relevant Authority in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.
  2. For the purposes of determining whether a Financial Distress Event has occurred the credit rating of the Monitored Company shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated the Monitored Company at or below the applicable Credit Rating Threshold.

1. **What happens if there is a financial distress event**
   1. In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if the Relevant Authority becomes aware of the Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and the Relevant Authority shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6 of this Annex 5.
   2. The Supplier shall and shall procure that the other Monitored Companies shall:
      1. at the request of the Relevant Authority meet the Relevant Authority as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) to review the effect of the Financial Distress Event on the continued performance of each Contract and delivery of the Deliverables in accordance each Call-Off Contract; and
      2. where the Relevant Authority reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1) that the Financial Distress Event could impact on the continued performance of each Contract and delivery of the Deliverables in accordance with each Call-Off Contract:
         1. submit to the Relevant Authority for its Approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within ten (10) Working Days of the initial notification (or awareness) of the Financial Distress Event); and
         2. provide such financial information relating to the Monitored Company as the Relevant Authority may reasonably require.
   3. If the Relevant Authority does not (acting reasonably) approve the draft Financial Distress Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to the Relevant Authority within five (5) Working Days of the rejection of the first or subsequent (as the case may be) drafts. This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by the Relevant Authority or referred to the Dispute Resolution Procedure.
   4. If the Relevant Authority considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not remedy the relevant Financial Distress Event, then it may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the Dispute Resolution Procedure.
   5. Following Approval of the Financial Distress Service Continuity Plan by the Relevant Authority, the Supplier shall:
      1. on a regular basis (which shall not be less than Monthly), review the Financial Distress Service Continuity Plan and assess whether it remains adequate and up to date to ensure the continued performance each Contract and delivery of the Deliverables in accordance with each Call-Off Contract;
      2. where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1, submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 4.5 and 4.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and
      3. comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).
   6. Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Relevant Authority and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.
   7. CCS shall be able to share any information it receives from the Buyer in accordance with this Paragraph with any Buyer who has entered into a Call-Off Contract with the Supplier.
2. **When CCS or the Buyer can terminate for financial distress** 
   1. CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:
      1. the Supplier fails to notify the Relevant Authority of a Financial Distress Event in accordance with Paragraph 3.4;
      2. The Relevant Authority and the Supplier fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 4.3 to 4.5; and/or
      3. the Supplier fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraph 4.6.3.
   2. If the Contract is terminated in accordance with Paragraph 5.1, Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply as if the Contract had been terminated under Clause 10.4.1.
3. **What happens If your credit rating is still good**
   1. Without prejudice to the Supplier’s obligations and CCS’ and the Buyer’s rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:
      1. the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and
      2. The Relevant Authority shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

(Security) Consultancy Security Schedule

*The security schedule is currently in draft and will be finalised within 30 days of contract signature.*

**Buyer Options**

**Risk assessment**

|  |  |  |
| --- | --- | --- |
| 1. The Buyer has assessed this Contract as: | 1. a standard consultancy agreement |  |
| 1. a higher-risk consultancy agreement |  |

**Relevant Certifications**

|  |  |  |
| --- | --- | --- |
| 1. Where the Buyer has assessed this Contract as a standard consultancy agreement, it requires the Supplier to be certified as compliant with: | 1. No certification required |  |
| 1. Cyber Essentials (or equivalent) |  |
| 1. Cyber Essentials Plus (or equivalent) |  |

**Buyer Security Policies**

|  |  |
| --- | --- |
| 1. The Buyer requires the Supplier to comply with the following policies relating to security management:  * [**List Buyer security policies with which the Supplier and Sub-contractors must comply**] |  |

**Staff Vetting Procedure**

|  |  |
| --- | --- |
| 1. The Buyer requires a Staff Vetting Procedure other than BPSS. Where the Buyer selects this option, the alternative Staff Vetting Procedure with which the Supplier must comply is:  * [**Set out any Buyer Security Vetting Procedure with which the Supplier and Sub-contractors must comply**] |  |

**Supplier obligations**

Where the Buyer has assessed this Contract as a higher-risk consultancy agreement, the Supplier must comply with all requirements in this Schedule 16 (Security).

Where the Buyer has assessed this Contract as a standard consultancy agreement, the Supplier must comply with this Schedule 16 (Security), other than:

the requirement to be certified as compliant with ISO/IEC 27001:2022 (or equivalent) under Paragraph 7.1(b); and

the requirement to undertake security testing of the Supplier Information Management System in accordance with Paragraph 9 of Appendix 1.

the requirement to produce a Security Management Plan in accordance with Paragraph 9.

**Definitions**

In this Schedule 16 (Security):

|  |  |
| --- | --- |
| * 1. **“Anti-virus Software”** | 1. means software that:    * 1. protects the Supplier Information Management System from the possible introduction of Malicious Software;      2. scans for and identifies possible Malicious Software in the Supplier Information Management System;      3. if Malicious Software is detected in the Supplier Information Management System, so far as possible:         1. prevents the harmful effects of the Malicious Software; and         2. removes the Malicious Software from the Supplier Information Management System. |
| * 1. **“Breach of Security”** | * 1. means the occurrence of:      1. any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data;      2. the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or      3. any part of the Supplier System ceasing to be compliant with the Relevant Certifications;      4. the installation of Malicious Software in the Supplier System:      5. any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the Supplier System; and      6. includes any attempt to undertake the activities listed in sub-Paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:         1. was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or         2. was undertaken, or directed by, a state other than the United Kingdom; |
| * 1. **“Buyer Equipment”** | * 1. means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System. |
| * 1. **“Certification Default”** | * 1. means the occurrence of one or more of the circumstances listed in Paragraph 7.4. |
| * 1. **“Certification Rectification Plan”** | * 1. means the plan referred to in Paragraph 7.5(a). |
| * 1. **“Certification Requirements”** | * 1. means the information security requirements set out in Paragraph 7. |
| 1. **“CHECK Scheme”** | 1. means the NCSC’s scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks. |
| 1. **“CHECK Service Provider”** | 1. means a company which, under the CHECK Scheme:    * 1. has been certified by the National Cyber Security Centre;      2. holds "Green Light" status; and      3. is authorised to provide the IT Health Check services required by Paragraph 9 of the Security Requirements. |
| 1. **“CHECK Team Leader”** | 1. means an individual with a CHECK Scheme team leader qualification issued by the NCSC. |
| 1. **“CHECK Team Member”** | 1. means an individual with a CHECK Scheme team member qualification issued by the NCSC. |
| * 1. **“Cyber Essentials”** | * 1. means the Cyber Essentials certificate issued under the Cyber Essentials Scheme. |
| * 1. **“Cyber Essentials Plus”** | * 1. means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme. |
| * 1. **“Cyber Essentials Scheme”** | * 1. means the Cyber Essentials scheme operated by the National Cyber Security Centre. |
| * 1. **“End-user Device”** | * 1. means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device provided by the Supplier or a Sub-contractor and used in the provision of the Services. |
| 1. **“Expected Behaviours”** | 1. means the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of <https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html>. |
| 1. **“Government Security Classification Policy”** | 1. means the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at [https://www.gov.uk/ government/publications/government-security-classifications](https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html). |
| * 1. **“Handle”** | * 1. means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data. |
| * 1. **“HMG Baseline Personnel Security Standard”** | * 1. means the employment controls applied to any individual member of the Supplier Staff that performs any activity relating to the provision or management of the Services, as set out in “HMG Baseline Personnel Standard”, Version 7.0, June 2024(<https://www.gov.uk/government/publications/government-baseline-personnel-security-standard> ), as that document is updated from time to time. |
| * 1. **“NCSC Device Guidance”** | * 1. means the National Cyber Security Centre’s document “Device Security Guidance”, as updated or replaced from time to time and found at <https://www.ncsc.gov.uk/collection/device-security-guidance>. |
| * 1. **“Privileged User”** | * 1. means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges. |
| * 1. **“Prohibited Activity”** | * 1. means the storage, access or Handling of Government Data prohibited by a Prohibition Notice. |
| * 1. **“Prohibition Notice”** | * 1. means a notice issued under Paragraph 1.2 of Appendix 1. |
| * 1. **“Relevant Certifications”** | * 1. means those certifications specified in Paragraph 7.1. |
| * 1. **“Relevant Convictions”** | * 1. means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Buyer may specify. |
| 1. **“Remote Location”** | 1. means a location other than a Supplier’s or a Sub-contractor’s Site. |
| 1. **“Remote Working”** | 1. means the provision or management of the Services by Supplier Staff from a location other than a Supplier’s or a Sub-contractor’s Site. |
| 1. **“Remote Working Policy”** | 1. the policy prepared and approved under Paragraph 3.8 of the Security Requirements under which Supplier Staff are permitted to undertake Remote Working. |
| 1. **“Security Controls”** | 1. means the security controls set out and updated from time to time in the Government Security Classification Policy, currently found at Paragraph 12 of <https://www.gov.uk/government/publications/government-security-classifications/guidance-15-considerations-for-security-advisors-html> |
| * 1. **“Security Management Plan”** | * 1. means the document prepared in accordance with the requirements of Paragraph 9. |
| * 1. **“Standard Contractual Clauses”** | * 1. means the standard data protection clauses specified in Article 46 of the United Kingdom General Data Protection Regulation setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area. |
| * 1. **“Supplier Information Management System”** | * 1. means:      1. those parts of the information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Services; and      2. the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources). |
| * 1. **“Sub-contractor Staff”** | * 1. means:      1. any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and      2. engaged in or likely to be engaged in:         1. the performance or management of the Services;         2. or the provision of facilities or services that are necessary for the provision of the Services. |
| * 1. **“UKAS”** | * 1. means the United Kingdom Accreditation Service. |
| 1. **UKAS-recognised Certification Body** | 1. means:    * 1. an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or      2. an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual recognition agreement recognising the technical equivalence of accredited conformity assessment. |

**Introduction**

This Schedule 16 (Security) sets out:

the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Contract to ensure the security of the Government Data, the Services and the Supplier Information Management System;

the assessment of this Contract as either a:

standard consultancy agreement; or

higher-risk consultancy agreement,

in Paragraph 1;

the Buyer’s access to the Supplier Staff and Supplier Information Management System, in Paragraph 6;

the Certification Requirements, in Paragraph 7;

in the case of higher-risk consultancy agreements, the requirements for a Security Management Plan in Paragraph 9.

the security requirements with which the Supplier and Sub-contractors must comply in Appendix 1.

**Principles of security**

The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Government Data and, consequently on the security of:

the Sites;

the Services; and

the Supplier’s Information Management System.

The Supplier is responsible for:

the security, confidentiality, integrity and availability of the Government Data when that Government Data is under the control of the Supplier or any of its Sub-contractors; and

the security of the Supplier Information Management System.

The Supplier must:

comply with the security requirements in Appendix 1; and

ensure that each Sub-contractor that Handles Government Data complies with the security requirements in Appendix 1.

Where the Supplier, a Sub-contractor or any of the Supplier Staff is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Sub‑contractors and Supplier Staff comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

**Access to Supplier Staff and Supplier Information Management System**

The Buyer may require, and the Supplier must provide the Buyer and its authorised representatives with:

access to the Supplier Staff;

access to the Supplier Information Management System to audit the Supplier and its Sub-contractors’ compliance with this Contract; and

such other information and/or documentation that the Buyer or its authorised representatives may reasonably require,

to assist the Buyer to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure

the security of the Government Data; and

the Supplier Information Management System are consistent with the representations in

the Security Management Plan.

The Supplier must provide the access required by the Buyer in accordance with Paragraph 6.1 within [ten] Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within [24 hours] of receipt of such request.

**Certification Requirements**

The Supplier shall ensure that, unless otherwise agreed by the Buyer, it is certified as compliant with:

in the case of a standard consultancy agreement the option chosen by the Buyer in Paragraph 1; or

in the case of a higher-risk consultancy agreement:

either:

an ISO/IEC 27001:2022 certification by a UKAS-Recognised Certification Body in respect of the Supplier Information Management System (or an equivalent certification); or

where the Supplier Information Management System is included within the scope of a wider ISO/IEC 27001:2022 certification (or an equivalent certification) that certification; and

Cyber Essentials Plus (or an equivalent certification) (“**Relevant Certifications”**).

Unless otherwise agreed by the Buyer, the Supplier must provide the Buyer with a copy of the Relevant Certifications before it begins to provide the Services.

The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications are:

currently in effect;

together, relate to the full scope of the Supplier Information System; and

are not subject to any condition that may impact the provision of the Services.

The Supplier must notify the Buyer promptly, any in any event within three Working Days of becoming aware that:

a Relevant Certification in respect of the Supplier Information Management System has been revoked or cancelled by the body that awarded it;

a Relevant Certification in respect of the Supplier Information Management System has expired and has not been renewed by the Supplier;

the Relevant Certifications, together, no longer apply to the full scope of the Supplier Information Management System or

the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a “**Certification Default**”).

Where the Supplier has notified the Buyer of a Certification Default under Paragraph 7.4:

the Supplier must, within ten working Days of the date in which the Supplier provided notice under Paragraph 7.4 (or such other period as the Parties may agree) provide a draft plan (a “**Certification Rectification Plan**”) to the Supplier setting out:

full details of the Certification Default, including a root cause analysis;

the actual and anticipated effects of the Certification Default;

the steps the Supplier will take to remedy the Certification Default;

the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

if the Buyer rejects the Certification Rectification Plan, the Buyer must within five Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph 7.5(b) will apply to the re-submitted plan;

the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Contract;

if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

**Government Data Handled using Supplier Information Management System**

The Supplier acknowledges that the Supplier Information Management System:

is intended only for the Handling of Government Data that is classified as OFFICIAL; and

is not intended for the Handling of Government Data that is classified as SECRET or TOP SECRET,

in each case using the Government Security Classification Policy.

The Supplier must:

not alter the classification of any Government Data; and

if it becomes aware that any Government Data classified as SECRET or TOP SECRET is being Handled using the Supplier Information Management System:

immediately inform the Buyer; and

follow any instructions from the Buyer concerning that Government Data.

The Supplier must, and must ensure that Sub-contractors and Supplier Staff, when Handling Government Data, comply with:

the Expected Behaviours; and

the Security Controls.

Where there is a conflict between the Expected Behaviours or the Security Controls and this Schedule 16 (Security) the provisions of this Schedule 16 (Security) shall apply to the extent of any conflict.

**Security Management Plan**

This Paragraph 9 applies only where the Buyer has assessed that this Contract is a higher-risk consultancy agreement.

1. **Preparation of Security Management Plan**

The Supplier shall document in the Security Management Plan how the Supplier and its Sub‑contractors shall comply with the requirements set out in this Schedule 16 (Security) and the Contract in order to ensure the security of the Government Data and the Supplier Information Management System.

The Supplier shall prepare and submit to the Buyer within [20] Working Days of the date of this Call-Off Contract, the Security Management Plan, which must include:

an assessment of the Supplier Information Management System against the requirements of this Schedule 16 (Security), including Appendix 1;

the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Government Data, the Buyer, the Services and/or users of the Services;

the Remote Working Policy (where the Supplier or a Sub-contractor proposes to allow Supplier Staff to work from a Remote Location); and

the following information in respect of each Sub-contractor:

the Sub-contractor’s:

legal name;

trading name (if any);

registration details (where the Sub-contractor is not an individual);

the Sites used by the Sub-contractor;

the Government Data Handled by the Sub‑contractor;

the Handling that the Sub-contractor will undertake in respect of the Government Data;

the measures the Sub-contractor has in place to comply with the requirements of this Schedule 16 (Security ).

The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to Handle Government Data; or

a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within [ten] Working Days of the date of the rejection, or such other period agreed with the Buyer.

1. **Updating Security Management Plan**

The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.

1. **Monitoring**

The Supplier shall notify the Buyer within [two] Working Days after becoming aware of:

a significant change to the components or architecture of the Supplier Information Management System;

a new risk to the components or architecture of the Supplier Information Management System;

a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;

* + 1. a change in the threat profile;

a significant change to any risk component;

a significant change in the quantity of Personal Data held within the Service;

a proposal to change any of the Sites from which any part of the Services are provided; and/or

an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

Within [ten] Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

Appendix 1: Security requirements

**Location**

Unless otherwise agreed with the Buyer, the Supplier must, and must ensure that its Sub‑contractors must, at all times, store, access or Handle Government Data either:

* + 1. in the United Kingdom; or
    2. in a location permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).

The Supplier must, and must ensure that its Subcontractors store, access or Handle Government Data in a facility operated by an entity where:

* + 1. the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);
    2. that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Schedule 16] (Security);
    3. the Supplier or Subcontractor has taken reasonable steps to assure itself that:
       1. the entity complies with the binding agreement; and
       2. the Subcontractor’s system has in place appropriate technical and organisational measures to ensure that the Sub-contractor will store, access, manage and/or Handle the Government Data as required by this Schedule 16 (Security);
    4. the Buyer has not given the Supplier a Prohibition Notice under Paragraph 1.3.

The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub‑contractors must not undertake or permit to be undertaken, the storage, access or Handling Government Data as specified in the notice (a “**Prohibited Activity**”).

* + 1. in any particular country or group of countries;
    2. in or using facilities operated by any particular entity or group of entities; or
    3. in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity (a “**Prohibition Notice**”).

Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant Activities affected by the notice, the Supplier must, and must procure that Sub-contractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.

**Physical Security**

The Supplier must ensure, and must ensure that Sub-contractors ensure, that:

* + 1. all locations at which Government Data is Handled (**Secure Locations**) have the necessary physical protective security measures in place to prevent unauthorised access, damage and interference, whether malicious or otherwise, to that Government Data;
    2. the operator of each Secure Location has prepared a physical security risk assessment and a site security plan for the Secure Location.

**Vetting, Training and Staff Access**

**Vetting before performing or managing Services**

The Supplier must not engage Supplier Staff, and must ensure that Sub-contractors do not engage Sub-contractor Staff, in any activity relating to the performance and management of the Services unless:

* + 1. That individual has passed the security checks listed in Paragraph 3.2; or
    2. The Buyer has given prior written permission for a named individual to perform a specific role.

For the purposes of Paragraph 3.1, the security checks are:

* + 1. the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:
       1. the individual’s identity;
       2. the individual’s nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;
       3. the individual’s previous employment history; and
       4. that the individual has no Relevant Convictions;
    2. national security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or
    3. such other checks for the Supplier Staff of Sub-contractors as the Buyer may specify.

**Exception for certain Sub-contractors**

Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Staff, it must:

* + 1. as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;
    2. provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor Staff will perform as the Buyer reasonably requires; and
    3. comply, at the Supplier’s cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Staff and the management of the Sub-contractor.

**Annual training**

The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Staff, complete and pass security training at least once every calendar year that covers:

* + 1. general training concerning security and data handling; and
    2. phishing, including the dangers from ransomware and other malware.

**Staff access**

The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Staff can access only the Government Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.

The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Staff no longer require access to the Government Data or any part of the Government Data, their access to the Government Data or that part of the Government Data is revoked immediately when their requirement to access Government Data ceases.

Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Staff’s access to the Government Data or part of that Government Data specified by the Buyer as soon as practicable and in any event within 24 hours of the request.

**Remote Working**

The Supplier must ensure, and ensure that Sub-contractors ensure, that:

* + 1. unless approved in writing by the Authority, Privileged Users do not undertake Remote Working;
    2. where the Authority permits Remote Working by Privileged Users, the Supplier ensures, and ensures that Sub-contractors ensure, that such Remote Working takes place only in accordance with any conditions imposed by the Authority.

Where the Supplier or a Sub-contractor wishes to permit Supplier Staff to undertake Remote Working, it must:

* + 1. prepare and have approved by the Buyer the Remote Working Policy in accordance with this Paragraph;
    2. undertake and, where applicable, ensure that any relevant Sub-contractors undertake, all steps required by the Remote Working Policy;
    3. ensure that Supplier Staff undertake Remote Working only in accordance with the Remote Working Policy;
    4. may not permit any Supplier Staff of the Supplier or any Sub-contractor to undertake Remote Working until the Remote Working Policy is approved by the Buyer.

The Remote Working Policy must include or make provision for the following matters:

* + 1. restricting or prohibiting Supplier Staff from printing documents in any Remote Location;
    2. restricting or prohibiting Supplier Staff from downloading any Government Data to any End-user Device other than an End-user Device that:
       1. is provided by the Supplier or Sub-contractor (as appropriate); and
       2. complies with the requirements set out in Paragraph 4 (*End-user Devices*);
    3. ensuring that Supplier Staff comply with the Expected Behaviours (so far as they are applicable);
    4. giving effect to the Security Controls (so far as they are applicable); and
    5. for each different category of Supplier Staff subject to the proposed Remote Working Policy:
       1. the types and volumes of Government Data that the Supplier Staff can Handle in a Remote Location and the Handling that those Supplier Staff will undertake;
       2. any identified security risks arising from the proposed Handling in a Remote Location;
       3. the mitigations, controls and security measures the Supplier or Sub-contractor (as applicable) will implement to mitigate the identified risks; and
       4. the business rules with which the Supplier Staff must comply.

The Supplier may submit a proposed Remote Working Policy to the Buyer for consideration at any time.

**End-user Devices**

The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Government Data is stored or Handled in accordance the following requirements:

* + 1. the operating system and any applications that store, Handle or have access to Government Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
    2. users must authenticate before gaining access;
    3. all Government Data must be encrypted using a encryption tool agreed to by the Buyer;
    4. the End-under Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
    5. the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Government Data;
    6. the Suppler or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Government Data on the device and prevent any user or group of users from accessing the device;
    7. all End-user Devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001:2018 certification issued by a UKAS-Recognised Certification Body (or equivalent certifications), where the scope of that certification includes the Services.

The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Contract.

Where there any conflict between the requirements of this Schedule 16(Security) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

**Encryption**

Unless Paragraph 5.2 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Government Data is encrypted:

* + 1. when stored at any time when no operation is being performed on it; and
    2. when transmitted.

Where the Supplier, or a Sub-contractor, cannot encrypt Government Data as required by Paragraph 5.1, the Supplier must:

* + 1. immediately inform the Buyer of the subset or subsets of Government Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
    2. provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;
    3. provide the Buyer with such information relating to the Government Data concerned, the reasons why that Government Data cannot be encrypted and the proposed protective measures as the Buyer may require.

The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Government Data.

This Paragraph applies where the Buyer has assessed that this Contract is a higher-risk consultancy agreement.

Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:

* + 1. the subset or subsets of Government Data not encrypted and the circumstances in which that will occur;
    2. the protective measure that the Supplier and/or Sub-contractor will put in please in respect of the unencrypted Government Data.

Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Government Data, either party may refer the matter to [be determined by an expert in accordance with the Dispute Resolution Procedure].

**Backup and recovery of Government Data**

The Supplier must ensure that the Supplier System:

backs up and allows for the recovery of Government Data to achieve the recovery point and recovery time objectives specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified; and

retains backups of the Government Data for the period specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified.

The Supplier must ensure the Supplier System:

* + 1. uses backup location for Government Data that are physically and logically separate from the rest of the Supplier System;
    2. the backup system monitors backups of Government Data to:
       1. identifies any backup failure; and
       2. confirm the integrity of the Government Data backed up;
    3. any backup failure is remedied promptly;
    4. the backup system monitors the recovery of Government Data to:
       1. identify any recovery failure; and
       2. confirm the integrity of Government Data recovered; and
    5. any recovery failure is promptly remedied.

**Access Control**

The Supplier must, and must ensure that all Sub-contractors:

* + 1. identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
    2. require multi-factor authentication for all user accounts that have access to Government Data or that are Privileged Users;
    3. allow access only to those parts of the Supplier Information Management System and Sites that those persons require;
    4. maintain records detailing each person’s access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.

The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:

* + 1. are accessible only from dedicated End-user Devices;
    2. are configured so that those accounts can only be used for system administration tasks;
    3. require passwords with high complexity that are changed regularly;
    4. automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive.

The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different passwords for their different accounts on the Supplier Information Management System.

The Supplier must, and must ensure that all Sub-contractors:

* + 1. configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and
    2. change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

**Malicious Software**

The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.

The Supplier shall ensure that such Anti-virus Software:

* + 1. prevents the installation of the most common forms of Malicious Software in the Supplier Information Management System;
    2. is configured to perform automatic software and definition updates;
    3. performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and
    4. where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.

If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

Any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Supplier, or a Sub‑contractor, to comply with this Paragraph 8 is a material Default.

**Security Testing**

This Paragraph applies only where the Buyer has assessed that this Contract is a higher-risk consultancy agreement.

**Note:** the definition of Supplier Information Management System includes those information and communications technology systems that Sub-contractors will use to assist or contribute to the Supplier providing the Services.

The Supplier must before providing the Services and when reasonably requested by the Buyer, either:

* + 1. provide details of any security testing undertaken by a CHECK Service Provider in respect of the Supplier Information Management System in the calendar year immediately preceding the Buyer’s request or the Effective Date (as appropriate), including:
       1. the parts of the Supplier Information Management System tested;
       2. a full, unedited and unredacted copy of the testing report; and
       3. the remediation plan prepared by the Supplier to address any vulnerabilities disclosed by the security testing; and
       4. the Supplier’s progress in implementing that remediation plan; or
    2. where no such testing was undertaken, conduct security testing of the Supplier Information Management System by:
       1. engaging a CHECK Service Provider and ensuring that the CHECK Service Provider uses a qualified CHECK Team Leader and CHECK Team Members to perform the testing;
       2. designing and implementing the testing so as to minimise its impact on the Supplier Information Management System and the delivery of the Services; and
       3. providing the Buyer with a full, unedited and unredacted copy of the testing report without delay and in any event within ten Working Days of its receipt by the Supplier.

The Supplier must remediate any vulnerabilities classified as “medium” or above in the security testing:

* + 1. before Handling Buyer data where the vulnerability is discovered before the Supplier begins to Handle Government Data;
    2. where the vulnerability is discovered when the Supplier has begun to Handle Government Data:
       1. by the date agreed with the Buyer; or
       2. where no such agreement is reached:

within five Working Days of becoming aware of the vulnerability and its classification where the vulnerability is classified as critical;

within one month of becoming aware of the vulnerability and its classification where the vulnerability is classified as high; and

within three months of becoming aware of the vulnerability and its classification where the vulnerability is classified as medium.

The Supplier must notify the Buyer immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as high or medium in a Security Test report within the time periods specified in Paragraph 9.3(b).

**Breach of Security**

If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours.

The Supplier must, upon becoming aware of a Breach of Security immediately take those steps identified in the Security Management Plan and all other reasonably steps necessary to:

* + 1. minimise the extent of actual or potential harm caused by such Breach of Security;
    2. remedy such Breach of Security to the extent possible;
    3. apply a tested mitigation against any such Breach of Security; and
    4. prevent a further Breach of Security in the future which exploits the same root cause failure.

If the Supplier becomes aware of a Breach of Security that impacts or has the potential to impact the Government Data, it shall:

notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours;

provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer’s satisfaction;

where the Law requires the Buyer to report a Breach of Security to the appropriate regulator provide such information and other input as the Buyer requires within the timescales specified by the Buyer; and

where the Breach of Security results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data, undertake any communication or engagement activities required by the Buyer with the individuals affected by the Breach of Security.

As soon as reasonably practicable and, in any event, within five Working Days, or such other period agreed with the Buyer, following the Breach of Security or attempted Breach of Security, provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

The Supplier must take the steps required by Paragraph 10.2 at its own cost and expense.

**Sub-contractors**

The Supplier must, before entering into a binding Sub‑contract with any Sub‑contractor:

* + 1. undertake sufficient due diligence of the proposed Sub‑contractor to provide reasonable assurance that the proposed Sub‑contractor can perform the obligations that this Schedule requires the Supplier ensure that the proposed Sub‑contractor performs;
    2. keeps adequate records of the due diligence it has undertaken in respect of the proposed Sub‑contractors; and
    3. provides those records to the Buyer on request.

**Third-party software and tools**

Before using any software or tool as part of the Supplier Information Management System, the Supplier must:

* + 1. perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that software or tool; and
    2. where there are any recognised security vulnerabilities, either:
       1. remedy vulnerabilities; or
       2. ensure that the design of the Supplier Information Management System mitigates those vulnerabilities;
    3. keep adequate records of the due diligence and efforts to remedy or mitigate identified vulnerabilities; and
    4. provide the Buyer with copies of those records on request.

The Supplier must ensure that all software used to provide the Services remains at all times in full security support, including any extended or bespoke security support.

**Deletion and return of Government Data**

The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Government Data held by the Supplier or Sub-contractor when requested to do so by the Buyer using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

Paragraph 13.1 does not apply to Government Data:

* + 1. that is Personal Data in respect of which the Supplier is a Controller;
    2. to which the Supplier has rights to Handle independently from this Contract; or
    3. in respect of which, the Supplier is under an obligation imposed by Law to retain.

The Supplier must, and must ensure that all Subcontractors, provide the Buyer with copies of any or all Government Data held by the Supplier or Subcontractor:

* + 1. when requested to do so by the Buyer; and

using the method specified by the Buyer.

# Annex 2– DVSA Security Requirements *The security schedule is currently in draft and will be finalised within 30 days of contract signature.*

## Introduction

* 1. Annex 2 sets out the Security and Confidentiality requirements that the Potential Provider and any subcontractors must comply with in delivery of the contract.
  2. The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:
     + 1. Authorities Security Representative: Graham Watts
       2. Phoenix’s Security Representative: Shaun Tosler.

## Definitions

* 1. In this Annex, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

|  |  |
| --- | --- |
| "Breach of Security" | the occurrence of:  any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including Confidential Information and DVSA information assets) used by DVSA and/or the Potential Provider in connection with this Contract; and/or  the loss and/or unauthorised disclosure of any information or data (including Confidential Information and DVSA information assets), including any copies of such information or data, used by DVSA and/or the Potential Provider in connection with this Contract,  in either case as more particularly set out in the Security Policy where DVSA has required compliance therewith in accordance with paragraph 3.1; |
| "Security Management Plan" | the Potential Provider's security management plan prepared pursuant to this Annex, a draft of which has been provided by the Potential Provider to DVSA and as updated from time to time. |

## Complying with security requirements and updates to them

* 1. The Potential Provider shall comply with the requirements in this Annex in respect of the Security Management Plan. The Potential Provider shall also comply with the DVSA Security Policy and shall ensure that the Security Management Plan produced by the Potential Provider fully complies with the DVSA Security Policy.
  2. Where the DVSA Security Policy applies the DVSA shall notify the Potential Provider of any changes or proposed changes to the DVSA Security Policy.
  3. If the Potential Provider believes that a change or proposed change to the DVSA Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the DVSA. In doing so, the Potential Provider must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.
  4. Until and/or unless a change to the Charges is agreed by the DVSA pursuant to the Variation Procedure the Potential Provider shall continue to provide the Deliverables in accordance with its existing obligations.

## Security Standards

* 1. The Potential Provider acknowledges that DVSA places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.
  2. The Potential Provider shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:
     1. is in accordance with the Law and this Contract;
     2. as a minimum demonstrates Good Industry Practice;
     3. meets any specific security threats of immediate relevance to the Deliverables and/or DVSA information assets; and
     4. where specified by DVSA, complies with the DVSA Security Policy and the DVSA ICT Policy;
     5. complies with relevant legislation, organisational and cross-Government policy and guidelines in relation to data and asset security including but not limited to Data Protection Act 2018, General Data Protection Regulation (UK GDPR 2018), HMG Security Policy Framework, Cabinet Office Minimum Cyber Security Standard (2018), National Cyber Security Centre Cloud Security Principles.
  3. The references to standards, guidance and policies contained or set out in Paragraph 4.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Potential Provider from time to time.
  4. In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Potential Provider should notify DVSA's Representative of such inconsistency immediately upon becoming aware of the same, and DVSA's Representative shall, as soon as practicable, advise the Potential Provider which provision the Potential Provider shall be required to comply with.

## Requirements

| ID | Title | Description |
| --- | --- | --- |
| Governance | | |
| GR01 | Named Contact | The Potential Provider must provide a single named point of contact at their organisation responsible for the security of their information systems.  **Shaun Tosler.** |
| GR02 | Security Policy | The Potential Provider shall ensure that they maintain an up-to-date security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable following the Start Date to the DVSA.  The Security Policy must include, at a minimum, security risk management (security risk assessment, incident response, evaluation and security roles and responsibilities), Potential Provider personnel integrity (recruitment, training, staff responsibilities, vetting, and disciplinary procedures), compliance with legislation, handling of information from creation to destruction or deletion, management of suspected/actual security breaches and business continuity arrangements.  **We maintain an Information security policy and manual as part of the ISO27001:2022 certification.** |
| GR03 | Certifications | The Potential Provider must be accredited against ISO 27001:2022 and commit to maintaining this for the duration of the contract.  The Potential Provider must currently hold a Cyber Essentials certification and maintain this for the duration of the contract.  **Confirmed.** |
| GR04 | Potential Provider Location | The Potential Provider must maintain a base of operations within the UK.  **Confirmed.** |
| GR05 | Data location | Should the Potential Provider desire to host DVSA data and information assets outside the UK or seek to transfer these outside of the UK they must first seek consent from the DVSA.  Should it not be practicable to host DVSA data and information assets in the UK then the DVSA has a preference that they are hosted either in:   1. The EEA 2. Countries with adequacy agreements (Andorra, Canada [commercial organisations only], Faroe Islands, Guernsey, Isle of Man, Japan [private-sector organisations only], Jersey, New Zealand, Switzerland and Uruguay).   If the Potential Provider seeks to host DVSA data or information assets outside of the UK, the EEA or the countries with adequacy agreements discussed then they will be required to complete a data transfer risk assessment which will be reviewed by DVSA.  No DVSA data or information assets may be hosted or transferred to the following states:   * Argentina, * Armenia, * Azerbaijan, * Belarus, * China (including Hong Kong and Macao), * Cyprus, * Egypt, * Estonia, * India, * Indonesia, * Iran, * Iraq, * Israel, * Jordan, * Kazakhstan, * Kuwait, * Kyrgzstan, * Latvia, * Lithuania, * Moldova, * Morocco, * North Korea, * Oman, * Pakistan, * Palestinian Territory, * Qatar, * Russia * Saudi Arabia, * Tajikistan, * Turkey, * Turkmenistan, * Ukraine, * United Arab Emirates, * Uzbekistan, * Yemen.   **Phoenix hosts its data within the UK, as we control our environment and any data it hosts. However, since many suppliers/vendors will be hosting DVSA’s data as it is covered by multiple software licenses, Phoenix cannot control the data residency and related controls, which falls under the vendor's responsibilities.** |
| GR06 | Security Management Plan | The Potential Provider must develop and maintain a Security Management Plan as described in Section 6.  **N/A, as this engagement is limited to providing software licenses and support. We maintain ISMS and Information Security Manual based on the ISO27001:2022 requirements.** |
| GR07 | Security Assurance | Where requested by DVSA the Potential Provider will support security assurance activities relating to IT systems used to provide the services in this contract including compliance with recommendations to remediate any identified risks.  The Potential Provider will facilitate engagement with any providers of software selected in delivery of this contract to allow DVSA to conduct security assurance activities.  **To be discussed.** |
| GR08 | Security Testing | The Potential Provider must ensure that any of their IT infrastructure involved in delivery of this contract undergoes security testing on an at least annual basis including an ITHC conducted by a CHECK-certified provider. Following testing the Potential Provider must implement a remediation action plan to resolve any identified vulnerabilities on a reasonable timescale. The results of these ITHCs must be provided to DVSA on request.  **Confirmed from Phoenix’s end only and not from the other vendors' side.** |
| GR09 | Security Audit | The Potential Provider must support DVSA in conducting audits of its compliance with security requirements on an at least annual basis and prior to implementation. Following a security audit the Potential Provider must develop a remediation action plan for any issues identified to be agreed with DVSA.  **Confirmed from Phoenix’s end only and not from the other vendors' side.** |
| GR10 | Personnel Security | All Potential Provider staff, including subcontractors, with access to DVSA data or information assets must hold either SC clearance or undergo a Baseline Personnel Security Standard (BPSS) check.  All Potential Provider staff with access to DVSA data or information assets or systems holding DVSA data or information assets shall undergo training on secure information management principles on an at least annual basis.  **Phoenix staff are BPSS checked.** |
| GR11 | Security of Purchased Software | The DVSA reserves the right to request that the providers of software selected by the Potential Provider sign a security agreement with DVSA detailing minimum security requirements prior to software deployment.  **N/A** |
| GR12 | Secure System Development Lifecycle | Should the Potential Provider develop any software to support delivery of this contract they must ensure that their development practices include security throughout the system development lifecycle aligned with NCSC guidance  This must also be applied to any suppliers of software selected by the Potential Provider (<https://www.ncsc.gov.uk/collection/cyber-security-design-principles>).  **N/A** |
| GR13 | Exit | On completion of the contract or decommissioning of the solution the Potential Provider must support DVSA in conducting migration activities and ensure that all storage devices are sanitised in line with best practice such as NIST 800-88 or NCSC guidance. On sanitisation the Potential Provider must provide DVSA with a certificate of sanitisation identifying the method used for sanitisation, the assets sanitised, the date on which they were sanitised and the signature of the individual responsible for sanitisation.  **N/A, as this engagement is limited to providing software licenses and support.** |
| GR14 | Test Data | DVSA data, information assets or data related to delivery of this contract must not be used in testing of the Potential Provider’s systems without explicit consent of DVSA.  **Confirmed from Phoenix’s end only and not from the other vendors' side.** |
| GR15 | Machine Learning Tools | DVSA data, information assets or data related to delivery of this contract must not be used in training of machine learning models by the Potential Provider without explicit consent of DVSA.  **Confirmed from Phoenix’s end only and not from the other vendors' side.** |
| GR16 | Third-Party Risk Management Processes | The Potential Provider must gain agreement from DVSA prior to granting access to DVSA data or information assets to any of their third parties. The Potential Provider must conduct security risk assessments on any of their third parties handling DVSA data or information assets, provide the results of these risk assessments to DVSA and implement remediation actions for any identified risks in consultation with DVSA  **Confirmed for Phoenix.** |
| GR17 | Change Management | The Potential Provider must inform DVSA of any major changes to their IT infrastructure that may impact on the secure handling of DVSA data or information assets.  **N/A Phoenix’s end. Phoenix will provide any information received from the other vendors.** |
| GR18 | Asset Management Processes | The Potential Provider must maintain an asset register for all IT assets and conduct annual audits to ensure that this remains accurate.  **N/A** |
| GR19 | Security Classification | The Potential Provider shall ensure that the Government Security Classification (GSC) Policy ([Government Security Classifications Policy June 2023.docx (publishing.service.gov.uk)](https://assets.publishing.service.gov.uk/media/649c38e006179b00113f745b/Government_Security_Classifications_Policy_June_2023.pdf)) rating is also applied when information and data is transmitted across all applicable networks and/or in line with DVSA requirements.  Handling of data marked OFFICIAL-SENSITIVE must ensure no removal or obfuscation of GSC classification in metadata.  **No Official-sensitive data is handled in this engagement. However, if any requirement to handle any sensitive information, we will discuss and work with DVSA to ensure proper controls in place.** |
| GR20 | Legislation | The Potential Provider shall ensure that they support the DVSA in meeting their legislative obligations including, but not limited to, those set out in:   * UK General Data Protection Regulations 2018 * Data Protection Act 2018 * Freedom of Information Act 2000 * Human Rights Act 1998 * Privacy & Electronic Communications Regulations 2006 (PECR) * Regulation of Investigatory Powers Act (2016) * The Investigatory Powers Act 2016   This includes assisting the DVSA in carrying out a data protection impact assessment and identifying and mitigating privacy risks to a level acceptable to the DVSA.  **Confirmed from Phoenix’s end only and not from the other vendors' side.** |
| GR21 | Secure by Design | The Potential Provider must consider, and, where appropriate, align with, the HMG Secure by Design Principles ([Secure by Design Principles - UK Government Security](https://www.security.gov.uk/guidance/secure-by-design/principles/)) in provision of services relating to this contract.  **N/A.**  **However, for any future requirement, we will discuss and work with DVSA to ensure proper controls in place.** |
| GR22 | Data Processing Requirements | Should there be a requirement for a supplier of software selected by the Potential Provider in delivery of this contract to process personal information for which DVSA is a data controller, the Potential Provider must support DVSA in provision of a data processing agreement with that supplier.  **Confirmed from Phoenix side.** |
| GR23 | Selected Software Security Questionnaire | On selection of software to fulfil requirements requested by DVSA the Potential Provider must complete a Selected Software Security Questionnaire for that software and the associated software supplier as described in Section 8 and provide this to DVSA for review. DVSA reserves the right to update this questionnaire as required over the course of the contract.  **Confirmed from Phoenix side.** |
| GR24 | Risk Ledger Profile | The Potential Provider must complete a profile on Risk Ledger (riskledger.com) within twenty (20) working days of the start date of the contract.  **Confirmed. Here is the link to the profile.**  <https://app.riskledger.com/p/shared/0f154c6e0d944ecf8c94f53601e0fc27> |
| Technical | | |
| TR01 | Access Controls | The Potential Provider’s information systems must be configured to ensure that only authorised users can gain access to them. All users must be uniquely identified and authenticated before being granted access to the Potential Provider’s information systems.  Access to any DVSA data or information assets processed by the Potential Provider’s information systems must be limited to those with a need to know and protected with industry standard access and authentication controls.  **Confirmed from Phoenix’s end only and not from the other vendors' side, as we don’t control their environment.** |
| TR02 | Privileged Access | Where a member of Potential Provider staff grants increased access privileges to Potential Provider information systems, those staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.  **Confirmed from Phoenix’s end only and not from the other vendors' side, as we don’t control their environment.** |
| TR03 | Encryption in Transit | Data in transit must be secured with industry best practice encryption techniques (such as TLS 1.2 or above) suitable for protection of OFFICIAL data.  **Confirmed from Phoenix’s end only and not from the other vendors' side, as we don’t control their environment.** |
| TR04 | Encryption at Rest | Data at rest must be secured with industry best practice encryption techniques suitable for protection of OFFICIAL data.  **Confirmed from Phoenix’s end only and not from the other vendors' side, as we don’t control their environment.** |
| TR05 | Key Management | Cryptographic keys managed by the Potential Provider must be managed effectively using a key management solution that facilitates rotation of secrets and keys in configurable timeframes.  **Confirmed from Phoenix’s end only and not from the other vendors' side, as we don’t control their environment.** |
| TR06 | Patch Management | The Potential Provider must maintain a patch management policy detailing at a minimum, the timeframes to apply security patches, and rollback plans in event of patch failure. This must be supplied to DVSA for review within 20 working days of contract award.  Patches must be tested on a non-production environment prior to deployment on live and DVSA must be informed of any expected downtime at least 24 hours in advance of patching. At a minimum the Potential Provider must ensure that patches are deployed within one period of a patching cycle.  **Confirmed from Phoenix’s end only, we hold Cyber Essentials Plus certification.** |
| TR07 | Logging and Monitoring | The Potential Provider must collect logs from all network devices and endpoints handling DVSA data or information assets and ensure that these are monitored to detect abnormal behaviour using a protective monitoring tool. The Potential Provider must implement processes to distinguish between security alerts and false positives and alerts should trigger incident response processes. The Potential Provider must ensure that access to logs collected for monitoring purposes is strictly controlled and that the logs are immutable.  **N/A for Phoenix, as this engagement is limited to providing software licenses and support.**  **For other vendors, please check the logging and monitoring requirements with them directly.** |
| TR08 | Security  Incident Management | The Potential Provider must document and maintain Security Incident Management Plans for the services included in this contract and provide these to DVSA within twenty (20) working days of the start date of the contract.  In the event of an incident affecting the confidentiality, integrity or availability of DVSA data or information assets the Potential Provider must notify DVSA within 24 hours including details of any mitigating and recovery actions that have taken place or are ongoing.  The Potential Provider must attempt to minimise the impact on DVSA data or information assets during an incident and seek to conduct mitigating activities in consultation with DVSA. On closure of a security incident the Potential Provider must contact DVSA identifying the root cause and steps taken to ensure that the incident cannot reoccur.  **Confirmed from Phoenix’s end only and not from the other vendors' side, as we don’t control their environment.** |
| TR09 | Backups | For any data relating to the delivery of this contract, the Potential Provider must conduct backups on a daily basis and store these securely in line with the requirements for live data. Backups must be retained for 6 months and allow restoration within 1 day. Restoration from backups must be tested on an at least annual basis and the results of the testing provided to DVSA for review.  **N/A, as this engagement is limited to providing software licenses and support.** |
| TR10 | Secure Configuration | The Potential Provider must ensure that any of their IT infrastructure involved in delivery of the service adheres to common industry standards including but not limited to:  • AWS/Microsoft/Google best practice security principles  • NCSC guidance and principles • NIST security and cybersecurity standards • OWASP • GDPR and DPA 2018   Any deviations from these must be brought to the attention of the DVSA during the design phase or as soon as identified thereafter.  **N/A to Phoenix, as this engagement is limited to providing software licenses and support.**  **Requirements are to be discussed for the other vendor's side, as we don’t control their environment.** |
| TR11 | Malware Protection | The Potential Provider must ensure that their information systems are protected with suitable malware protection tools and that these are updated regularly.  **Confirmed from Phoenix’s end only, and not from the other vendors' side, as we don’t control their environment.** |
| TR12 | Network Security | Potential Provider networks must be configured in a secure manner with network boundaries configured to prevent connections by unauthorised users and in line with industry best practice. Networks should be appropriately segregated into different trust zones based on sensitivity.  **Confirmed from Phoenix’s end only and not from the other vendors' side, as we don’t control their environment.** |
| TR13 | End User Device Security | Any end user devices used by the Potential Provider to deliver the service must be securely configured in line with NCSC guidance ([Platform Guides - NCSC.GOV.UK](https://www.ncsc.gov.uk/collection/device-security-guidance/platform-guides)).  **Confirmed from Phoenix’s end only and not from the other vendors' side, as we don’t control their environment.** |
| TR14 | Customer Separation | Information systems handling DVSA data or information assets must be logically separated from those handling data belonging to other customers.  **Confirmed from Phoenix’s end only and not from the other vendors' side, as we don’t control their environment.** |
| TR15 | Environments | The Potential Provider must maintain separate environments for development, testing and Live. These must be separated from each other. Live DVSA data should never enter the development or testing environments without explicit consent of DVSA.  **N/A** |

## Security Management Plan

* 1. **Introduction**
     1. The Potential Provider shall develop and maintain a Security Management Plan in accordance with this Annex. The Potential Provider shall thereafter comply with its obligations set out in the Security Management Plan.
  2. **Content of the Security Management Plan**
     1. The Security Management Plan shall:
     2. comply with the principles of security set out in Section 4 and any other provisions of this Contract relevant to security;
     3. identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Potential Provider;
     4. detail the process for managing any security risks from Subcontractors and third parties authorised by DVSA with access to the Deliverables, processes associated with the provision of the Deliverables, DVSA Premises, the Sites and any ICT, Information and data (including DVSA’s Confidential Information and any other DVSA information assets) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
     5. be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including DVSA Premises, the Sites, and any ICT, Information and data (including DVSA Confidential Information and any other DVSA information assets) to the extent used by the DVSA or the Potential Provider in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
     6. set out the security measures to be implemented and maintained by the Potential Provider in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;
     7. set out the plans for transitioning all security arrangements and responsibilities for the Potential Provider to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with the DVSA Security Policy; and
     8. be written in plain English in language which is readily comprehensible to the staff of the Potential Provider and DVSA engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Annex.
  3. **Development of the Security Management Plan**
     1. Within twenty (20)Working Days after the Start Date and in accordance with Paragraph 6.4, the Potential Provider shall prepare and deliver to DVSA for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.
     2. If the Security Management Plan submitted to DVSA in accordance with Paragraph 6.3.1, or any subsequent revision to it in accordance with Paragraph 6.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Annex. If the Security Management Plan is not Approved, the Potential Provider shall amend it within ten (10) Working Days of a notice of non-approval from DVSA and re-submit to DVSA for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to DVSA. If DVSA does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.
     3. DVSA shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 6.3.2. However a refusal by DVSA to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 6.2 shall be deemed to be reasonable.
     4. Approval by DVSA of the Security Management Plan pursuant to Paragraph 6.3.2 or of any change to the Security Management Plan in accordance with Paragraph 6.4, shall not relieve the Potential Provider of its obligations under this Annex.
  4. **Amendment of the Security Management Plan**
     1. The Security Management Plan shall be fully reviewed and updated by the Potential Provider at least annually to reflect:
     2. emerging changes in Good Industry Practice;
     3. any change or proposed change to the Deliverables and/or associated processes;
     4. any change to the DVSA Security Policy;
     5. any new perceived or changed security threats; and
     6. any reasonable change in requirements requested by DVSA.
     7. The Potential Provider shall provide DVSA with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to DVSA. The results of the review shall include, without limitation:
     8. suggested improvements to the effectiveness of the Security Management Plan;
     9. updates to the risk assessments; and
     10. suggested improvements in measuring the effectiveness of controls.
     11. Subject to Paragraph 6.4.4, any change or amendment which the Potential Provider proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 6.4.1, a request by DVSA or otherwise) shall be subject to the Variation Procedure.
     12. DVSA may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

## Security breach

1. 1. Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.
   2. Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 7.1, the Potential Provider shall:
      1. immediately take all reasonable steps (which shall include any action or changes reasonably required by DVSA) necessary to:
      2. minimise the extent of actual or potential harm caused by any Breach of Security;
      3. remedy such Breach of Security to the extent possible and protect the integrity of DVSA and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;
      4. prevent an equivalent breach in the future exploiting the same cause failure; and
      5. as soon as reasonably practicable provide to DVSA, where DVSA so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by DVSA.
   3. In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the DVSA Security Policy (where relevant in accordance with paragraph 3.1) or the requirements of this Annex, then any required change to the Security Management Plan shall be at no cost to DVSA.

## Selected Software Security Questionnaire

| ID | Question |
| --- | --- |
| SQ01 | Does the selected software supplier hold a valid ISO 27001 certification? **Yes** |
| SQ02 | Does the selected software supplier hold a valid Cyber Essentials or Cyber Essentials Plus certification? **Yes** |
| SQ03 | Does the selected software supplier have a single named contact for security? If so, provide details. **Yes, Shaun Tosler.** |
| SQ04 | Will any DVSA data or information assets be processed, accessed or stored outside of the UK? If so, provide details on location, how DVSA data or information assets will be processed, accessed and stored and who by. **Phoenix hosts its data within the UK** |
| SQ05 | Does the selected solution include provisions for secure access and authentication controls? Does the selected solution support multifactor authentication? If so, provide details. **N/A to Phoenix.** |
| SQ06 | Where DVSA data and information assets will be processed, accessed or stored by the selected solution or by the software supplier will it be encrypted in transit and at rest in line with industry best practice? **N/A to Phoenix.** |
| SQ07 | Where DVSA data and information assets will be accessed, stored or processed by the selected solution or by the software supplier will it be logically separated from data and information assets belonging to other customers? **N/A to Phoenix.** |
| SQ08 | Does the selected software supplier follow a secure software development lifecycle? **N/A to Phoenix.** |
| SQ09 | Does the selected software supplier monitor security logs to detect potential security incidents? Does the selected software supplier maintain a security incident management policy? **N/A to Phoenix.** |
| SQ10 | Will the selected software supplier staff have access to any DVSA data and information assets processed, accessed or stored by any provided solution? **N/A to Phoenix.** |
| SQ11 | Does the selected software supplier use customer data in testing or in training of machine learning models? **N/A to Phoenix.** |
| SQ12 | Has the selected software supplier implemented an anti-malware solution to protect any environment that will process or store DVSA data or information assets? **Yes.** |