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

# Order Form

| | |
|---|---|
| CALL-OFF REFERENCE: | C2991 |
| THE BUYER: | Intellectual Property Office (IPO) |
| BUYER ADDRESS | REDACTED |
| THE SUPPLIER: | Health Assured Limited |
| SUPPLIER ADDRESS: | REDACTED |
| REGISTRATION NUMBER: | 06314620 |
| DUNS NUMBER: | 21-007-1628 |

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 14 August 2023. It's issued under the Framework Contract with the reference number RM6182 Occupational Health, Employee Assistance Programmes and Eye Care Services, Lot 3 for the provision of an Employee Assistance Programme to the IPO.

CALL-OFF LOT(S):

Lot 3

CALL-OFF INCORPORATED TERMS:

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) RM6182.

3. The following Schedules in equal order of precedence:

    - Joint Schedules for RM6182
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 10 (Rectification Plan)
        - Joint Schedule 11 (Processing Data)

    - Call-Off Schedules for RM6182
        - Call-Off Schedule 3 (Continuous Improvement)
        - Call-Off Schedule 5 (Pricing Details)
        - Call-Off Schedule 7 (Key Supplier Staff)
        - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
        - Call-Off Schedule 9 (Security)
        - Call-Off Schedule 14 (Service Levels)
        - Call-Off Schedule 18 (Background Checks)
        - Call-Off Schedule 20 (Call-Off Specification)

4. CCS Core Terms (version 3.0.8)
5. Joint Schedule 5 (Corporate Social Responsibility) RM6182
6. 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

]

None

| | |
|---|---|
| CALL-OFF START DATE: | 1 September 2023 |
| CALL-OFF EXPIRY DATE: | 31 August 2026 |
| CALL-OFF INITIAL PERIOD: | 3 Years |
| CALL-OFF OPTIONAL EXTENSION: | Two distinct periods of 12 Months at the sole discretion of the Authority (subject to approvals and budget) together with the written agreement of both parties |

CALL-OFF DELIVERABLES

See details in Call-Off Schedule 20 (Call-Off Specification)

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 £10,000.00 estimated charges in the first 12 months of the Contract.

CALL-OFF CHARGES

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

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

Payment will only be made on satisfactory delivery of the agreed services. Before payment, any invoices that are received must include a detailed breakdown of the work completed, the associated costs and a quote reference number. All invoices must quote a relevant IPO Purchase Order and Contract reference number and be emailed to payables@ipo.gov.uk. Payment will be made within 30 days of receipt of invoice.

BUYER'S INVOICE ADDRESS:

REDACTED

BUYER'S AUTHORISED REPRESENTATIVE

REDACTED

BUYER'S ENVIRONMENTAL POLICY

Our energy use - Intellectual Property Office - GOV.UK (www.gov.uk)

BUYER'S SECURITY POLICY

Security Policy for Contractors.pdf

SUPPLIER'S AUTHORISED REPRESENTATIVE

REDACTED

SUPPLIER'S CONTRACT MANAGER

REDACTED

PROGRESS REPORT FREQUENCY

On the first Working week of each quarter month, unless requested otherwise

PROGRESS MEETING FREQUENCY

Quarterly on the first Working week of each quarter

KEY STAFF

Not applicable

KEY SUBCONTRACTOR(S)

Not applicable

COMMERCIALLY SENSITIVE INFORMATION

Descriptions of the Service, details of the Call Off Charges and any breakdown of said Charges provided to the Buyer are considered Commercially Sensitive Information for the duration of this Agreement.

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)

**Signed by an authorised signatory for and behalf of the Supplier**

Supplier_Signature

REDACTED

REDACTED

22 August 2023

**For and on behalf of the Buyer**

Contracting_Authority_Signature

REDACTED

REDACTED

22 August 2023

# Call-Off Schedules for RM6182

# Call-Off Schedule 3 (Continuous Improvement)

### Buyer's Rights

i. 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.

7. **Supplier's Obligations**

i. 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.

ii. 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.

iii. 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:

i. identifying the emergence of relevant new and evolving technologies;

ii. 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);

iii. 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

iv. 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.

iv. 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.

v. 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.

vi. 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.

vii. 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.

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

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

ii. 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.

ix. 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.

x. 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.

xi. 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.

xii. 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)

REDACTED

# Call-Off Schedule 5 (Pricing Details)

Head Count Cost:

REDACTED

Costs for Counselling Services and Therapeutic Interventions:

REDACTED

Costs for Trauma and Critical Incident Support:

REDACTED

Costs for Health and Wellbeing Promotion and Awareness:

REDACTED

REDACTED

Costs for Consultancy & Clinical Supervision:

REDACTED

Costs for Mediation Services:

REDACTED

Costs for Health Kiosks:

REDACTED

Structured Support Costs:

REDACTED

# Call-Off Schedule 7 (Key Supplier Staff)

1.1 The Annex 1 to this Schedule 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.

# Annex 1- Key Roles

| Key Role | Key Staff | Contract Details |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

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

## Definitions

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

| | |
|---|---|
| **"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; |
| **"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; |
| **"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; and |
| **"Supplier's Proposals"** | ● has the meaning given to it in Paragraph 6.3 of this Schedule; |

## 8. BCDR Plan

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

ii. 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:

i. ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and

ii. the recovery of the Deliverables in the event of a Disaster

iii. The BCDR Plan shall be divided into three sections:

i. Section 1 which shall set out general principles applicable to the BCDR Plan;

ii. Section 2 which shall relate to business continuity (the **"Business Continuity Plan"**); and

iii. Section 3 which shall relate to disaster recovery (the **"Disaster Recovery Plan"**).

iv. 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.

## 9. General Principles of the BCDR Plan (Section 1)

i. Section 1 of the BCDR Plan shall:

i. set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;

ii. 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;

iii. contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;

iv. 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;

v. 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;

vi. 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;

vii. provide for documentation of processes, including business processes, and procedures;

viii. set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;

ix. identify the procedures for reverting to "normal service";

x. 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;

xi. identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and

xii. 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.

ii. The BCDR Plan shall be designed so as to ensure that:

i. the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;

ii. the adverse impact of any Disaster is minimised as far as reasonably possible;

iii. it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and

iv. it details a process for the management of disaster recovery testing.

iii. 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.

iv. 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.

## 10. Business Continuity (Section 2)

i. 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:

i. 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

ii. 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.

ii. The Business Continuity Plan shall:

i. address the various possible levels of failures of or disruptions to the provision of Deliverables;

ii. 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;

iii. 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

iv. set out the circumstances in which the Business Continuity Plan is invoked.

## 11. Disaster Recovery (Section 3)

i. 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.

ii. The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:

i. loss of access to the Buyer Premises;

ii. loss of utilities to the Buyer Premises;

iii. loss of the Supplier's helpdesk or CAFM system;

iv. loss of a Subcontractor;

v. emergency notification and escalation process;

vi. contact lists;

vii. staff training and awareness;

viii. BCDR Plan testing;

ix. post implementation review process;

x. 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;

xi. 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;

xii. access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

xiii. testing and management arrangements.

## 12. Review and changing the BCDR Plan

i. The Supplier shall review the BCDR Plan:

  i. on a regular basis and as a minimum once every six (6) Months;

  ii. within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 7; and

  iii. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

## 13. Testing the BCDR Plan

i. The Supplier shall test the BCDR Plan:

   i. regularly and in any event not less than once in every Contract Year;

   ii. in the event of any major reconfiguration of the Deliverables

   iii. at any time where the Buyer considers it necessary (acting in its sole discretion).

ii. 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.

iii. 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.

iv. 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.

v. The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:

   i. the outcome of the test;

   ii. any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

   iii. the Supplier's proposals for remedying any such failures.

vi. 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.

## 14. Invoking the BCDR Plan

i. 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.

15. **Circumstances beyond your control**

i. 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.

# Call-Off Schedule 9 (Security)

**Long Form Security Requirements**

**Definitions**

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

| | |
|---|---|
| **"Breach of Security"** | means the occurrence of:<br>any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or<br>the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,<br>in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d; |
| **"ISMS"** | the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and |
| **"Security Tests"** | tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security. |

## 16. Security Requirements

i. 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.

ii. The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

iii. The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

i. TBC - Security representative of the Buyer

ii. TBC - Security representative of the Supplier

iv. The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

v. Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

vi. The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.

vii. The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

viii. The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

## 17. Information Security Management System (ISMS)

i. The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.

ii. The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

iii. The Buyer acknowledges that;

i. If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be

an extant ISMS covering the Services and their implementation across the Supplier's estate; and

ii. Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.

iv. The ISMS shall:

i. if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;

ii. meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;

iii. at all times provide a level of security which:

1. is in accordance with the Law and this Contract;
2. complies with the Baseline Security Requirements;
3. as a minimum demonstrates Good Industry Practice;
4. where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;
5. complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework)
6. takes account of guidance issued by the Centre for Protection of National Infrastructure (https://www.cpni.gov.uk)
7. complies with HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm)
8. meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;
9. addresses issues of incompatibility with the Supplier's own organisational security policies; and
10. complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

iv. document the security incident management processes and incident response plans;

v. document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

vi. be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

v. Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 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 Supplier from time to time.

vi. In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

vii. If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall 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 the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

viii. Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

## 18. Security Management Plan

i. Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

ii. The Security Management Plan shall:

  i. be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);

  ii. comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;

  iii. identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

  iv. detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;

  v. unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier 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;

  vi. set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and 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 Schedule (including the requirements set out in Paragraph 3.4);

  vii. demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for

example, ‘platform as a service’ offering from the G-Cloud catalogue);

viii. set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

ix. set out the scope of the Buyer System that is under the control of the Supplier;

x. be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

xi. be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

iii. If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall 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 the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

iv. Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

19. **Amendment of the ISMS and Security Management Plan**

i. The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:

i. emerging changes in Good Industry Practice;

ii. any change or proposed change to the Supplier System, the Deliverables and/or associated processes;

iii. any new perceived or changed security threats;

iv. where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;

v. any new perceived or changed security threats; and

vi. any reasonable change in requirement requested by the Buyer.

ii. The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

i. suggested improvements to the effectiveness of the ISMS;

ii. updates to the risk assessments;

iii. proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

iv. suggested improvements in measuring the effectiveness of controls.

iii. Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.

iv. The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or 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.

## 20. **Security Testing**

i. The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

ii. The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.

iii. Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

iv. Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

v. If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

## 21. **Complying with the ISMS**

i. The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.

ii. If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.

iii. If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of

ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

## 22. Security Breach

i. Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

ii. Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

   i. immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

      1. minimise the extent of actual or potential harm caused by any Breach of Security;

      2. remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;

      3. apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

      4. prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

      5. supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

      6. as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach

of Security, including a root cause analysis where required by the Buyer.

iii. 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 ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

23. **Vulnerabilities and fixing them**

i. The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

ii. The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

  i. the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and

  ii. Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

iii. The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

  i. the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

  ii. the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or

  iii. the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

iv. The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6

Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

i. where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

ii. is agreed with the Buyer in writing.

v. The Supplier shall:

i. implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

ii. ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

iii. ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

iv. pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;

v. from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

vi. propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

vii. remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and

viii. inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

vi. If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

vii. A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

**Part B – Annex 1:**

**Baseline security requirements**

**Handling Classified information**

- The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

- **End user devices**
  - When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre (“NCSC”) to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").
  - Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a ‘known good’ state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

- **Data Processing, Storage, Management and Destruction**
  - The Supplier and Buyer recognise the need for the Buyer’s information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

- The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).
- The Supplier shall:
  - provide the Buyer with all Government Data on demand in an agreed open format;
  - have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;
  - securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and
  - securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

- **Ensuring secure communications**
  - The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.
  - The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

- **Security by design**
  - The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.
  - When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (https://www.ncsc.gov.uk/section/products-services/ncsc-certification) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

- **Security of Supplier Staff**
  - Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.
  - The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

- The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.
- All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.
- Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier 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.

- **Restricting and monitoring access**

  - The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

- **Audit**

  - The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:
    - Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.
    - Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.
  - The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.
  - The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

# Call-Off Schedule 14 (Service Levels)

## Definitions

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

| | |
|---|---|
| **"Amber Service Level Performance Measure"** | shall be the amber service level performance measure as set out against the relevant Service Level Performance Criterion in the Annex to Part A of this Schedule; |
| **"Critical Service Level Failure"** | means a failure to meet a Red Service Level Performance Measure for a Critical Service Level defined in the Order Form; |
| **"Green Service Level Performance Measure"** | shall be the green service level performance measure as set out against the relevant Service Level Performance Criterion in the Annex to Part A of this Schedule; |
| **"Red Service Level Performance Measure"** | shall be the red service level performance measure as set out against the relevant Service Level Performance Criterion in the Annex to Part A of this Schedule; |
| **"Service Credits"** | ● 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"** | ● has the meaning given to it in the Order Form; |
| | ● |
| **"Service Level Failure"** | ● means a failure to meet the Service Level Performance Measure in respect of a Service Level as follows:<br>▪ the Supplier's performance of any Critical Service Level is reported as failing to meet the Red Service Level Performance Measure in a given Service Period;<br>▪ the Supplier's performance of a single Service Level is reported as failing to meet the Red Service Level Performance Measure for that Service Level twice or more in any three (3) consecutive Service Periods; |

- the Supplier's performance of a single Service Level is reported as failing to meet the Red Service Level Performance Measure for that Service Level four (4) times or more in any twelve (12) consecutive Service Periods; and
- the Supplier's performance of a single Service Level is reported as failing to meet the Amber Service Level Performance Measure for that Service Level six (6) times or more in any twelve (12) consecutive Service Periods.

| | |
|---|---|
| **"Service Level Performance Measure"** | ● A Red Service Level Performance Measure, an Amber Service Level Performance Measure or a Green Service Level Performance Measure as set out against the relevant Service Level in the Annex to Part A of this Schedule; and |
| **"Service Level Threshold"** | ● shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule. |

- **What happens if you don't meet the Service Levels**
  - The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.
  - 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.
  - 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.
  - A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:
    - the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or
    - the Service Level Failure:
      - exceeds the relevant Service Level Threshold;
      - has arisen due to a Prohibited Act or wilful Default by the Supplier;
      - results in the corruption or loss of any Government Data; and/or

- results in the Buyer being required to make a compensation payment to one or more third parties; and/or

- the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

- 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:

  - 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;

  - 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

  - there is no change to the Service Credit Cap.

- **Critical Service Level Failure**

On the occurrence of a Critical Service Level Failure:

- any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and

- 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:

1.1 is likely to or fails to meet any Service Level Performance Measure; or

1.2 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:

i. 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;

ii. instruct the Supplier to comply with the Rectification Plan Process;

iii. if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or

iv. 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).

**2. Service Credits**

2.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

2.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

# Annex A to Part A: Services Levels and Service

**LOTS 1, 2 AND 4 ONLY - BASELINE SERVICE LEVELS FOR OCCUPATIONAL HEALTH SERVICES:**

| | | Service Level Performance Measure | | | | |
|---|---|---|---|---|---|---|
| Service Level Performance Criterion | Description | Service Level– Fail<br><br>RED | Service Level – Warning<br><br>AMBER | Service Level – Pass<br><br>GREEN | Service Credit Payable (%) | Critical Service Level |
| **Online Portal** | Online Portal to be available fifty two (52) weeks a year, Monday to Friday 08:00 to 18:00, excluding Public and Bank Holidays, except for agreed | <98% | >= 98% and < 100% | 100% | | Critical Service Level |

| | | | | | | |
|---|---|---|---|---|---|---|
| | downtime and maintenance which will be agreed with the Contracting Authorities at least seventy two (72) hours in advance of such work being carried.<br><br>Note: Some Contracting Authorities may require Services provided outside of these core hours and this will be agreed at Call Off contract | | | | | |
| **Telephone Support Services** | All telephone support line Services to be available Monday to Friday 08:00 to 18:00, fifty-two (52) weeks a year (or as defined by the Contracting Authorities) excluding public and bank holidays. | < 98% | >= 98% and < 100% | 100% | | Critical Service Level |
| | Occupational Health Physicians and Occupational Health Advisors to be available Monday to Friday 08:00 to 18:00, fifty two (52) weeks a year (or | < 98% | >= 98% and < 100% | 100% | | Critical Service Level |

| | | | | | | |
|---|---|---|---|---|---|---|
| | as defined by the Contracting Authorities) excluding public and bank holidays | | | | | |
| | All calls to be answered within five (5) rings | < 97% | >= 97% and < 98% | >= 98% | | |
| | All telephone messages and emails to be responded to within 24 hours | <97% | >= 98% and < 98% | >= 98% | | |
| **Case Management** | Occupational Health Advisor or Occupational Health Physician face to face consultation to be held and report to be provided within 15 working days of Contracting Authorities Personnel referral (including confirmation of appointment to the employee and line manager) | <97% | >= 97% and < 99% | >= 99% | | |
| | Occupational Health Advisor telephone consultation to be held and report to be delivered within four (4) working | <98% | >= 98% and < 100% | 100% | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | days of Contracting Authorities Personnel referral | | | | | |
| | Occupational Health Physician telephone consultation to be held and report to be delivered within seven (7) working days of Contracting Authorities Personnel referral | <98% | >= 98% and < 100% | 100% | | |
| | All written case reports to be right first time (with correct level of information and details) | <98% | >= 98% and < 100% | 100% | | |
| | Notification to the Contracting Authorities of an employee failing to attend appointment within one (1) working day of appointment being missed. | <100% | | 100% | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | On-site Occupational Health professionals to be available at the times agreed, including scheduled replacement Supplier Personnel. | <100% | | 100% | | |
| | File opinion to be delivered to the Contracting Authorities within five (5) working days on receipt of request. | <98% | >= 98% and < 100% | 100% | | |
| | Single case conferences to take place within 5 working days of request of Contracting Authorities | <98% | >= 98% and < 100% | 100% | | |
| | Multiple case conference (including collation of referrals) to take place within ten (10) working days of request | <98% | >= 98% and < 100% | 100% | | |
| **Further Medical Evidence** | Further Medical Evidence report requested from a specialist or General Practitioner | < 100% | | 100% | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | within two (2) days of the need having been identified by the Supplier | | | | | |
| **Ill Health retirements** | Medical opinion to support ill health retirement applications to be delivered within ten (10) working days of request | <97% | >= 97% and < 100% | 100% | | |
| **Health Surveillance and Fitness for Task** | All health surveillance, monitoring and specialist fit for task assessments and reports to be completed within ten (15) working days of referral. | <97% | >= 97% and < 100% | 100% | | Critical Service Level |
| | All paper based screening or assessments to be completed within three (3) working days of referral | <98% | >= 98% and < 100% | 100% | | |
| | All surveillance and assessments scheduled on a Contracting Authority's annual plan to be completed on time | <97% | >= 97% and < 99% | >= 99% | | |
| **Pre-Appointment and Pre-Enrolment Checks** | Delivery of report to Contracting Authorities following online screening within | <97% | >= 97% and < 99% | >= 99% | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | twenty four (24) hours | | | | | |
| | Occupational Health Adviser written opinion following online assessment to be delivered to the Contracting Authorities within two (2) working days | <98% | >= 98% and < 100% | 100% | | |
| | Telephone assessment of Contracting Authorities Personnel within three (3) working days of request. | <95% | >= 95% and < 99% | >=99% | | |
| | Face to face Contracting Authorities Personnel assessment within five (5) working days of request. | <95% | >= 95% and < 99% | >=99% | | |
| | Written opinion following telephone and face-to-face assessment to be be recived by Contracting Authorities within two (2) working days of the assessment. | <95% | >= 95% and < 99% | >=99% | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Physiotherapy** | Physiotherapy telephone assessment within four (4) working days of request | <97% | > = 97% and < 99% | >=99% | | |
| | Appointment and first face-to-face physiotherapy session to take place within seven (7) calendar days of referral | <97% | > = 97% and < 99% | >=99% | | |
| | Report delivered to Contracting Authorities within two (2) working days of completion of treatment | <97% | > = 97% and < 99% | >=99% | | |
| **Assessments** | For all Contracting Authorities Personnel assessments listed below : ten (15) working days from referral to delivery of report:<br><br>Workplace / Workstation Assessments<br><br>Occupational Therapy<br><br>Specialist assessments for sight and hearing<br><br>Dyslexia assessment<br><br>Specialist assessments | < 97% | > = 97% and < 99% | > = 99% | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | for disabled employees<br><br>Support Worker assessment | | | | | |
| **Complaints** | All customer Complaints to be acknowledged within one (1) Working Day of receipt | < 97% | > = 97% and < 99% | > = 99% | | |
| | Customer complaints to be resolved within ten (10) working days | < 97% | > = 97% and < 99% | > = 99% | | |
| **Customer Satisfaction** | All customer satisfaction surveys to meet agreed target measures | < 90% | > = 90% and < 95% | > = 95% | | |
| **Contract Management** | All invoices right first time, provided with supporting Data and received at the agreed times | < 97% | > = 97% and < 99% | > = 99% | | |
| | Account management support available Monday to Friday 8am -6pm with responses to queries from the Contracting Authorities within one (1) Working Day | < 97% | > = 97% and < 99% | > = 99% | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Management Information** | Management Information delivered at agreed periods with Contracting Authorities (defined at Call Off stage) | <100% | | 100% | | |
| | All ad hoc and urgent MI in relation to Freedom of Information requests, Minister's questions and Parliamentary Questions will be provided within the timelines outlined for each request by the Contracting Authorities | <100% | | 100% | | |

**LOTS 1 AND 3 ONLY: BASELINE SERVICE LEVELS FOR EMPLOYEE ASSISTANCE PROGRAMMES:**

| | | **Service Level Performance Measure** | | | | |
|---|---|---|---|---|---|---|
| **Service Level Performance Criterion** | **Description** | **Service Level– Fail**<br>**RED** | **Service Level – Warning**<br>**AMBER** | **Service Level – Pass**<br>**GREEN** | **Service Credit Payable (%)** | **Critical Service Level** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Telephone Support Services** | All telephone support line Services to be available twenty four (24) hours a day, seven (7) days a week, three hundred and sixty five (365) days a year | < 98% | >= 98% and < 100% | 100% | | Critical Service Level |
| | Urgent or 'red flag' cases will be matched immediately for telephone support | <100% | | 100% | | Critical Service Level |
| | All calls to be answered within five (5) rings | < 97% | >= 97% and < 98% | >= 98% | | |
| | Call abandonment rate to be less than two (2)% | <97% | >= 98% and < 100% | >= 99% | | |
| | Initial call back to Contracting Authorities Personnel following triage to take place within two (2) hours | <98% | >= 98% and < 100% | 100% | | |
| | All queries not requiring counselling Services to be | <97% | >= 97% and < 98% | >= 98% | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | completed within twenty four (24) hours. | | | | | |
| **Online Portal** | Online Portal to be available twenty four (24) hours a day, seven (7) days a week, three hundred and sixty five (365) days a year a day except for agreed downtime and maintenance which will be agreed with the Contracting Authorities at least seventy two (72) hours in advance of such work being carried out. | <97% | >= 98% and < 99% | >= 99% | | |
| **Counselling Services** | Counselling Services to be available twenty four (24) hours a day, seven (7) days a week, three hundred and sixty five | <100% | | 100% | | Critical Service Level |

| | | | | | | |
|---|---|---|---|---|---|---|
| | (365) days a year | | | | | |
| | Urgent or red flag cases will have first face to face counselling session offered within twenty four hours of first contact (if need determined) | <100% | | 100% | | Critical Service Level |
| | All counselling appointments (telephone, e-counselling or face to face) to be arranged within 48 hours of first contact | < 98% | >= 98% and < 100% | 100% | | |
| | Initial counselling session to take place within 5 days of first contact | <97% | >= 98% and < 99% | >= 99% | | |
| | Where the need for a fast track referral to counselling has been identified by the Supplier, the appointment | < 98% | >= 98% and < 100% | 100% | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | shall be booked within two (2) days of referral | | | | | |
| | Face-to-face counselling appointments to be offered within 1 hour's travelling distance by public transport of Contracting Authorities Personnel home office location | <97% | >= 98% and < 99% | >= 99% | | |
| **Trauma and Critical Incident Support** | Where critical incident procedures have been invoked, all employees (including those overseas) must have access to designated telephone support within two (2) hours of notification | < 100% | | 100% | | Critical Service Level |
| | A workplace site presence with the appropriate number of | < 100% | | 100% | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | skilled Supplier Personnel available within forty eight (48) hours | | | | | |
| **Complaints** | All complaints to be acknowledged within one (1) Working Day of receipt | < 97% | > = 97% and < 99% | > = 99% | | |
| | All Complaints to be updated at an interval of every two (2) Working Days | < 97% | > = 97% and < 99% | > = 99% | | |
| **Customer Satisfaction** | All customer satisfaction surveys to meet agreed target measures | < 90% | > = 90% and < 95% | > = 95% | | |
| **Contract Management** | All invoices right first time, provided with supporting data and received at the agreed times | < 97% | > = 97% and < 99% | > = 99% | | |
| | Account management support available Monday to | < 97% | > = 97% and < 99% | > = 99% | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Friday 8am - 6pm with responses to queries from the Contracting Authorities within one (1) Working Day | | | | | |
| **Management Information** | Management Information delivered at agreed periods with Contracting Authorities (defined at Call Off stage) | <100% | | 100% | | |
| | All ad hoc and urgent MI in relation to Freedom of Information requests, Minister's questions and Parliamentary Questions will be provided within the timelines outlined for each request by the Contracting Authorities | <100% | | 100% | | |

# Credits Table

The Service Credits shall be calculated on the basis of the following formula:

| | | |
|---|---|---|
| Formula: x% (Service Level Performance Measure) - x% (actual Service Level performance) | = | x% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer |
| Worked example: 98% (e.g. Service Level Performance Measure requirement for accurate and timely billing Service Level) - 75% (e.g. actual performance achieved against this Service Level in a Service Period) | = | 23% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer] |

# Part B: Performance Monitoring

**3. Performance Monitoring and Performance Review**

3.1 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.

3.2 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:

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

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

3.2.3 details of any Critical Service Level Failures;

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

3.2.5 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

3.2.6 such other details as the Buyer may reasonably require from time to time.

3.3 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:

3.3.1 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;

3.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and

3.3.3 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.

3.4 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.

3.5 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.

## 4. Satisfaction Surveys

4.1 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 18 (Background Checks)

**When you should use this Schedule**

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

24. **Definitions**

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

25. **Relevant Convictions**

i. 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.

ii. Notwithstanding Paragraph 2.1.1 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):

1. carry out a check with the records held by the Department for Education (DfE);
2. conduct thorough questioning regarding any Relevant Convictions; and
3. 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

Any applicable

# 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

| | |
|---|---|
| Project Title | Provision of Employee Assistance Programme |
| Project Term – Months | 3 years with an option to extend for a 1-year plus a further 1-year extension (3+1+1) |

## 1. SUMMARY

**1.1** We require this service to complement our Staff counselling service and Mental Health First Aiders – this will be additional support for the IPO

**1.2** An Employee Assistance Program (EAP) is a confidential workplace service that helps employees deal with work-life stressors, family issues, financial concerns, relationship problems, and even drug or legal concerns. It can often help workers remain productive at work.

## 2. BACKGROUND TO THE IPO

**2.1** The Intellectual Property Office (IPO) - an operating name of the Patent Office - is an Executive Agency of the Department of Science, Innovation and Technology (DSIT). It aims to stimulate innovation and enhance the international competitiveness of British industry and commerce. It offers customers an accessible, high quality, value for money system both nationally and internationally, for granting intellectual property rights.

**2.2** The IPO is a highly successful organisation which, over its 155-year history, has adapted its approach and services to meet changing demands. Its core business and products deliver high quality, cost effective Intellectual Property (IP) rights to customers and its success in these core areas is tied to a much wider range of activities, such as awareness-raising and enforcement. Its customers operate within both the UK and global economies. Further information about the IPO can be found on its website at: www.ipo.gov.uk

## 3. BACKGROUND TO THE REQUIREMENT

**3.1** There is evidence to suggest by adopting an Employee Assistance Program and providing support can maintain a productive and effective working environment. The primary goal of an EAP is to ensure the mental health of employees so that they can consistently contribute to the IPO. As part of the Corporate Plan at the IPO we have said:

***3.2*** *"We will ensure that people suffering from mental ill health are aware of the range of IPO support services, including launching a new employee assisting programme".*

## 4. DEFINITIONS

| Expression/Acronym | Definition |
|---|---|
| IPO | Intellectual Property Office |
| DSIT | Department of Science, Innovation and Technology |
| EAP | Employee Assistance Programme |
| CBT | Cognitive Behavioural Therapy |

## 5 AIMS AND OBJECTIVES

**5.1** The aim of the introduction of an Employee Assistance Program is to support our employees that may need help with various reasons including any work-life stressors or family concerns.

**5.2** The aim is support employees in addition to our Staff Counsellors and Mental Health First Aiders with a confidential service that helps the individual to develop coping skills to deal with any problems they encounter whilst remaining productive in work.

## 6 THE REQUIREMENT

**6.1** As a minimum the IPO require:

**6.1.1** 24-hour helpline - personal problems that affect health and wellbeing.

**6.1.2** Face to face referral – options both IPO's offices at REDACTED, REDACTED or any other premises that the IPO operate from throughout the duration of the contract.

**6.1.3** 24-hour helpline - personal problems that affect health and wellbeing.

**6.1.4** CBT trained staff Ideally (but this is not essential).

**6.1.5** Quickly respond to queries and calls as per the SLA's at Section 8.

**6.1.6** Access to MI so we can monitor how much the service is used

**6.1.7** Access to skills training availability on an ad hoc basis

**6.2** Financial Wellbeing Scheme - The Supplier shall provide an on-line financial education service and a range of products and services aimed at improving employees' financial well-being

**6.3** Comprehensive telephone helplines available 24 hours a day, 7 days a week, 365 days per year providing eligible persons with immediate telephone support including, but not limited to:

6.3.1 Work related issues including management, stress, workplace relationships, bullying and harassment.

6.3.2 Anxiety, stress, depression, low self-esteem, anger management.

6.3.3 Family, Marital and relationship issues.

6.3.4 Substance and alcohol misuse/dependency.

6.3.5 Bereavement.

6.3.6 Retirement.

6.3.7 Domestic abuse.

6.3.8 Health, and critical illness.

6.3.9 Lifestyle, exercise, diet, and general wellbeing.

6.3.10 Personal legal information.

**6.4** Medical information (available Monday to Friday, between 9am and 5pm).

**6.5** Online health and wellbeing portal such as REDACTED which provides access to extensive well-being resources including videos and webinars.

**6.6** Access to the 'My Healthy Advantage' mobile app, which provides a wealth of resources including mood trackers, mini health checks, four week plans and direct access to the EAP services.

**6.7** Up to six structured telephone and online counselling sessions, per issue, per year for the employee, partner or spouse and dependents (between the ages of 16-24 in full time education).

**6.8** Up to six face to face counselling sessions, per issue, per year for the employee including applied CBT.

**6.9** Electronic promotional materials, with hard copy available upon request.

**6.10** The Supplier shall provide telephone support for relevant Authorised Users with the authority to invoke critical incident support to provide immediate advice and recommendations regarding appropriate actions to support those affected. Any request made from the Customer or any eligible person to the Supplier shall be authorised in writing.

**6.11 Access to Whistleblowing Listening Service**

**6.12** The Supplier shall provide the Customer on a quarterly basis (within 15 working days of month end) with information regarding the number and types of calls analysed by book of business where appropriate and such other information it reasonably requires at the frequency and in the format agreed between the Parties from time to time.

**6.13 Additional Services:**

**6.14** Additional Services are to be provided on an ad-hoc basis upon receipt of a request and will be subject to the fees contained within the Appendix D – Price Schedule.

**6.15 Ad-Hoc Critical Incident Support**

**6.16** The Supplier shall provide Critical Incident Stress Management ("CISM") on site via a fully trained trauma counsellor or counselling team within 24 to 48 hours of a written request from the customer.

**6.17 Workshops**

**6.18** The Supplier shall provide workshops where trainers will refer back to the Supplier Services to encourage eligible persons to seek support through the

helpline. For eligible persons to gain the most from the workshops, we recommend a maximum of 20 eligible persons per session, with each workshop lasting 90 minutes to two hours.

**6.19 Mental Health First Aid Training**

**6.20** The Supplier shall provide fully certified training that follows the internationally recognised Mental Health First Aid England (Adult) course. Attendees will be provided with complimentary resources, including a mental health first aid manual, a workbook, and a "Z card" that can be used to identify mental health first aiders in the workplace. All Authorised Users who successfully complete the course will be a qualified mental health first aider.

**6.21 Informal Employee Referrals**

**6.22** If a manager feels that an employee would benefit from using the services directly, they can recommend the services to them as an additional source of help and guidance for any problems they may be experiencing.

**6.23 Formal Employee Referrals**

**6.24** To formally refer an employee, the manager will need to follow a set procedure, initiating the referral through the Supplier EAP Helpline referral route. It is important that such referrals have an initial clinical assessment of the situation. The counselling will then be provided either by telephone or face to face depending on the needs and preference of the employee.

**7. PROJECT MILESTONES**

**7.1** The potential provider will note the following project milestones

| Milestone | Description | Timeframe |
|---|---|---|
| 1 | Start-up meeting via Microsoft Teams | Within 1 week of contract award |
| 2 | Provision of expert counselling and support Services to Intellectual Property Office | From start of the contract to expiration of the contract |
| 3 | Management Information regarding the number and types of calls analysed by book of business where appropriate and such other information the IPO might reasonably require | Quarterly - from start of the contract to expiration of the contract |

**8.1 SERVICE LEVELS & CUSTOMER SERVICE**

**8.2** The Authority will measure the quality of the Supplier's delivery by:

| KPI/SLA | Service Area | KPI/SLA Description | Target |
|---|---|---|---|
| 1 | Quality of Services | The Supplier shall exercise reasonable s care and diligence in performance of all obligations performed under or in connection with the Contract. | 100% |

| | | | |
|---|---|---|---|
| 2 | Service Availability | The Supplier shall ensure that the Services, including the necessary Supplier Staff, are available to all users | 24 hours a day, 7 days a week and 365 days a year (366 for the 2024 'leap year', unless agreed otherwise in advance |
| 3 | Service Availability | The Supplier shall make the Services available to all groups outlined in the Framework Contract | 100% |
| 4 | Service Delivery | Attendance at relationship meetings each quarter (or at another interval as agreed by both parties) | 100% |
| 5 | Accuracy /Timelines | Accurate and timely billing of Customer | at least 98% at all times |
| 6 | Availability | Access to customer support | at least 98% at all times |
| 7 | Availability/ Timelines | Complaints Handling | At least 98% at all times |
| 8 | Quality | All helpline calls to be answered within 10 seconds | at least 95% at all times |
| 9 | Quality | Call abandonment rate | less than 1% |
| 10 | Services Availability | Initial call-backs to take place within 1 hour | at least 98% at all times |
| 11 | Services Availability | All counselling cases to be matched to a counsellor within 2 working days | at least 98% at all times |

## 9. OUTPUTS

**9.1** Management information data will be required initially 6-month basis to monitor uptake of the new service**.**

## 10. TIMINGS

**10.1** The EAP services will be delivered in line with the SLA's and timescales outlined with this specification document.

**10.2** REDACTED

## 11. RESOURCES

**11.1** The Supplier must be able to scale counsellor and support staff resources appropriately to ensure timely delivery of contract requirements while also maintaining an appropriate balance between such scaling and the cost of the EAP services to the IPO.

**12. VOLUMES**

**12.1** The IPO does not guarantee that the Supplier will be given any volume of work throughout the duration of the Contract**.**

**13. SECURITY REQUIREMENTS & CONFIDENTIALITY**

**13.1** Confidentiality: The Potential Provider will comply with clause 15 of the contract core terms and conditions in respect of all work carried out for the customer.

**14. SUSTAINABILITY**

**14.1** The IPO has a responsibility to act and to support nature, the environment, and its vital contributions to biodiversity. The Supplier is required to act in sustainable manner in the delivery of the Contract, particularly in terms of eliminating waste, reducing travel, and minimising energy consumption. The Supplier must comply with all current legislation regarding sustainability and legislation introduced or amended during the period of the contract pertaining to this.

**14.2** This must include compliance with the Modern Slavery Act 2015 and the Climate Change Act 2008.

**14.3** The Supplier must consider their carbon footprint in allocating and deploying resources to undertake requirement.

**15. CONTINUOUS IMPROVEMENT**

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

**15.2** The Supplier should present new ways of working to the Authority during quarterly Contract review meetings.

**15.3** Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

**16. PAYMENT**

**16.1** Payment will only be made on satisfactory delivery of the agreed services.

**16.2** Before payment, any invoices that are received must include a detailed breakdown of the work completed, the associated costs and a quote reference number.

**16.3** All invoices must quote a relevant IPO Purchase Order and Contract reference number and be emailed to REDACTED

**16.4** Payment will be made within 30 days of receipt of invoice.

# Joint Schedules for RM6182

# Joint Schedule 1 (Definitions)

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.

1.1 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.

1.2 In each Contract, unless the context otherwise requires:

1.2.1 the singular includes the plural and vice versa;

1.2.2 reference to a gender includes the other gender and the neuter;

1.2.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Central Government Body;

1.2.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.2.5 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**";

1.2.6 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;

1.2.7 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;

1.2.8 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;

1.2.9 references to **"Paragraphs"** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;

1.2.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;

1.2.11 the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract;

1.2.12 where the Buyer is a Central Government Body it shall be treated as contracting with the Crown as a whole;

1.2.13 any reference in a Contract which immediately before Exit Day is a reference to (as it has effect from time to time):

(a) 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

(b) 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

1.2.14 unless otherwise provided, references to "**Buyer**" shall be construed as including Exempt Buyers; and

1.2.15 unless otherwise provided, references to "**Call-Off Contract**" and "**Contract**" shall be construed as including Exempt Call-off Contracts.

1.3 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:<br>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);<br>● 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;<br>● verify the Open Book Data; |

| | |
|---|---|
| | ● verify the Supplier's and each Subcontractor's compliance with the applicable Law;<br>● 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;<br>● 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;<br>● 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;<br>● review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract;<br>● 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;<br>● 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<br>● verify the accuracy and completeness of any Management Information delivered or required by the Framework Contract; |
| **"Auditor"** | the Buyer's internal and external auditors;<br>● the Buyer's statutory or regulatory auditors;<br>● the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office;<br>● HM Treasury or the Cabinet Office;<br>● any party formally appointed by the Buyer to carry out audit or similar review functions; and<br>● 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:<br>a) Government Department;<br>b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);<br>c) Non-Ministerial Department; or<br>d) 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:<br>a) applicable Start Date; or<br>b) the Effective Date<br>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 GDPR; |
| **"Core Terms"** | CCS' standard terms and conditions for common goods and services which govern how Supplier 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:<br>e) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Work Day, of engaging the Supplier Staff, including:<br>i) base salary paid to the Supplier Staff;<br>ii) employer's National Insurance contributions;<br>iii) pension contributions;<br>iv) car allowances;<br>v) any other contractual employment benefits; |

| | |
|---|---|
| | vi) staff training;<br>vii) work place accommodation;<br>viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and<br>ix) reasonable recruitment costs, as agreed with the Buyer;<br>f) 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;<br>g) 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<br>h) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables;<br>but excluding:<br>i) Overhead;<br>j) financing or similar costs;<br>k) 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;<br>l) taxation;<br>m) fines and penalties;<br>n) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and<br>o) non-cash items (including depreciation, amortisation, impairments and movements in provisions); |
| **"CRTPA"** | the Contract Rights of Third Parties Act 1999; |
| **“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"** | the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of personal data and privacy; (iii) all applicable Law about the Processing of personal data and privacy; |

| | |
|---|---|
| **“Data Protection Liability Cap”** | the amount specified in the Framework Award Form; |
| **"Data Protection Officer"** | has the meaning given to it in the GDPR; |
| **"Data Subject"** | has the meaning given to it in the 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 the 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:<br>a) 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<br>b) is required by the Supplier in order to provide the Deliverables; and/or<br>c) 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:<br>a) the Expiry Date (as extended by any Extension Period exercised by the Relevant Authority under Clause 10.1.2); or<br>b) 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:<br>i) in the first Contract Year, the Estimated Year 1 Charges; or<br>ii) in the any subsequent Contract Years, the Charges paid or payable in the previous Call-off Contract Year; or<br>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:<br>a) eligible to use the Framework Contract; and<br>b) is entering into an Exempt Call-off Contract that is not subject to (as applicable) any of:<br>i) the Regulations;<br>ii) the Concession Contracts Regulations 2016 (SI 2016/273);<br>iii) the Utilities Contracts Regulations 2016 (SI 2016/274);<br>iv) the Defence and Security Public Contracts Regulations 2011 (SI 2011/1848); |

| | |
|---|---|
| | v) the Remedies Directive (2007/66/EC);<br>vi) Directive 2014/23/EU of the European Parliament and Council;<br>vii) Directive 2014/24/EU of the European Parliament and Council;<br>viii) Directive 2014/25/EU of the European Parliament and Council; or<br>ix) 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; |
| **"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, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under a Contract and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by the Affected Party, including:<br>a) riots, civil commotion, war or armed conflict;<br>b) acts of terrorism; |

| | |
|---|---|
| | c) acts of a Central Government Body, local government or regulatory bodies;<br>d) fire, flood, storm or earthquake or other natural disaster,<br>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 OJEU Notice; |
| **"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); |
| **"GDPR"** | the General Data Protection Regulation (Regulation (EU) 2016/679); |
| **"General Anti-Abuse Rule"** | e) the legislation in Part 5 of the Finance Act 2013 and; and |

| | |
|---|---|
| | f) 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 taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply; |
| **"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:<br>i) are supplied to the Supplier by or on behalf of the Authority; or<br>ii) 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; |
| **"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: |

| | |
|---|---|
| | a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract;<br><br>b) details of the cost of implementing the proposed Variation;<br><br>c) 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;<br><br>d) a timetable for the implementation, together with any proposals for the testing of the Variation; and<br><br>e) 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:<br><br>(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:<br><br>(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;<br><br>(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;<br><br>(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;<br><br>(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;<br><br>(e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;<br><br>(f) where that person is a company, a LLP or a partnership:<br><br>(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;<br><br>(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;<br><br>(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<br><br>(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<br><br>(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"** | a) 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;<br><br>b) 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<br><br>c) 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 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; |
| **"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:<br>a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or |

| | |
|---|---|
| | b) 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<br><br>c) 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,<br><br>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; |
| **"LED"** | Law Enforcement Directive (Directive (EU) 2016/680); |
| **"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 when two (2) MI Reports are not provided in any rolling six (6) month period |
| **"MI Failure"** | means when an MI report:<br><br>a) contains any material errors or material omissions or a missing mandatory field; or<br><br>b) is submitted using an incorrect MI reporting Template; or |

| | |
|---|---|
| | c) 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"** | 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<br>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;<br>but shall not include the Supplier's Existing IPR; |
| **"Occasion of Tax Non–Compliance"** | where:<br>any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of:<br>i) 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;<br>ii) 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<br>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:<br>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;<br>**5.** operating expenditure relating to the provision of the Deliverables including an analysis showing:<br>iii) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables;<br>iv) 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;<br>v) a list of Costs underpinning those rates for each grade, being the agreed rate less the Supplier Profit Margin; and<br>vi) Reimbursable Expenses, if allowed under the Order Form;<br>**6.** Overheads;<br>**7.** all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables;<br>**8.** the Supplier Profit achieved over the Framework Contract Period and on an annual basis;<br>**9.** 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;<br>**10.** 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<br>**11.** 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 GDPR; |
| **"Personal Data Breach"** | has the meaning given to it in the 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 GDPR; |
| **"Processor"** | has the meaning given to it in the GDPR; |
| **"Processor Personnel"** | all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract; |
| **"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"** | a) 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:<br>vii) induce that person to perform improperly a relevant function or activity; or<br>viii) reward that person for improper performance of a relevant function or activity;<br>b) 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<br>c) committing any offence:<br>ix) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or<br>x) under legislation or common law concerning fraudulent acts; or<br>xi) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or<br>d) 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. |
| **"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"** | a) the Supplier's plan (or revised plan) to rectify it's breach using the template in Joint Schedule 10 (Rectification Plan) which shall include:<br>b) full details of the Default that has occurred, including a root cause analysis;<br>c) the actual or anticipated effect of the Default; and<br>d) 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:<br>a) 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<br>b) 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"** | a) 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);<br>b) 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<br><br>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; |
| **"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:<br>a) the Deliverables are (or are to be) provided; or<br>b) 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:<br>a) 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; |

| | |
|---|---|
| | b) standards detailed in the specification in Schedule 1 (Specification);<br>c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time;<br>d) 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:<br>a) provides the Deliverables (or any part of them);<br>b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or<br>c) 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"** | a) 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;<br>b) 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;<br><br>c) 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:<br>Achieve a Milestone by its Milestone Date;<br><br>26. provide the Goods and/or Services in accordance with the Service Levels ; and/or<br><br>27. 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; |
| **"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:<br>a) for the Testing of the Deliverables; and<br>b) 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 –<br>(i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; an<br>(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); |
| **"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"** | 8.0 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")<br>And<br>[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:<br>. [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] |

. 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]

28. Words and expressions in this Variation shall have the meanings given to them in the Contract.

29. 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)

**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:
  - the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
  - the Call-Off Contract Effective Date in respect of the Additional Insurances.
- The Insurances shall be:
  - maintained in accordance with Good Industry Practice;
  - (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;
  - taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
  - maintained for at least six (6) years after the End Date.
- 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.

- **How to manage the insurance**

- Without limiting the other provisions of this Contract, the Supplier shall:
  - 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;
  - promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
  - 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.

- **What happens if you aren't insured**
    - 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.
    - 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.
- **Evidence of insurance you must provide**
    - 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.
- **Making sure you are insured to the required amount**
    - 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.
- **Cancelled Insurance**
    - 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.
    - 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.
- **Insurance claims**
    - 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.

- 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.
- Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 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:

i. professional indemnity insurance or medical malpractice 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);

ii. public 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); and

iii. 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).

# Joint Schedule 4 (Commercially Sensitive Information)

### What is the Commercially Sensitive Information?

iv. 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.

v. 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).

vi. 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 |
|---|---|---|---|
| 1 | 21 August 2023 | Descriptions of the Service, details of the Call Off Charges and any breakdown of said Charges provided to the Buyer are considered Commercially Sensitive Information for the duration of this Agreement. | Indefinite |

# Joint Schedule 5 (Corporate Social Responsibility)

### What we expect from our Suppliers

vii. In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)

viii. CCS expects its Suppliers and Subcontractors to meet the standards set out in that Code. In addition, CCS expects its Suppliers and Subcontractors to comply with the Standards set out in this Schedule.

ix. The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

30. **Equality and Accessibility**

i. In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:

i. eliminate discrimination, harassment or victimisation of any kind; and

ii. advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

31. **Modern Slavery, Child Labour and Inhumane Treatment**

**"Modern Slavery Helpline"** means the mechanism for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at https://www.modernslaveryhelpline.org/report or by telephone on 08000 121 700.

i. The Supplier:

i. shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;

ii. shall not require any Supplier Staff or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;

iii. warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.

iv. warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offenses anywhere around the world.

v. shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offenses anywhere around the world.

vi. shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;

vii. shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;

viii. shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;

ix. shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;

x. shall not use or allow child or slave labour to be used by its Subcontractors;

xi. shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

## 32. **Income Security**

i. The Supplier shall:

i. ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;

ii. ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

iii. not make deductions from wages:

1. as a disciplinary measure
2. except where permitted by law; or
3. without expressed permission of the worker concerned;

iv. record all disciplinary measures taken against Supplier Staff; and

v. ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

## 33. **Working Hours**

i. The Supplier shall:

i. ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;

ii. that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;

iii. ensure that use of overtime used responsibly, taking into account:

- the extent;
- frequency; and
- hours worked;

by individuals and by the Supplier Staff as a whole;

ii. The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

iii. Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

- this is allowed by national law;
- this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;
- appropriate safeguards are taken to protect the workers' health and safety; and
- the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

iv. All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

34. **Sustainability**

i. The supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at:

https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs

# Joint Schedule 10 (Rectification Plan)

| Request for [Revised] Rectification Plan | | | |
|---|---|---|---|
| Details of the Default: | [Guidance: Explain the Default, with clear schedule and clause references as appropriate] | | |
| Deadline for receiving the [Revised] Rectification Plan: | [add date (minimum 10 days from request)] | | |
| Signed by [CCS/Buyer] : | | Date: | |
| Supplier [Revised] Rectification Plan | | | |
| Cause of the Default | [add cause] | | |

| | | | |
|---|---|---|---|
| Anticipated impact assessment: | [add impact] | | |
| Actual effect of Default: | [add effect] | | |
| Steps to be taken to rectification: | Steps | Timescale | |
| | 1. | [date] | |
| | 2. | [date] | |
| | 3. | [date] | |
| | 4. | [date] | |
| | […] | [date] | |
| Timescale for complete Rectification of Default | [X] Working Days | | |
| Steps taken to prevent recurrence of Default | Steps | Timescale | |
| | 1. | [date] | |
| | 2. | [date] | |
| | 3. | [date] | |
| | 4. | [date] | |
| | […] | [date] | |
| Signed by the Supplier: | | Date: | |
| Review of Rectification Plan [CCS/Buyer] | | | |
| Outcome of review | [Plan Accepted] [Plan Rejected] [Revised Plan Requested] | | |
| Reasons for Rejection (if applicable) | [add reasons] | | |
| Signed by [CCS/Buyer] | | Date: | |

# Joint Schedule 11 (Processing Data)

## Status of the Controller

The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA. A Party may act as:

"Controller" in respect of the other Party who is "Processor";

"Processor" in respect of the other Party who is "Controller";

"Joint Controller" with the other Party;

"Independent Controller" of the Personal Data where there other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

**Where one Party is Controller and the other Party its Processor**

Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

a systematic description of the envisaged Processing and the purpose of the Processing;

an assessment of the necessity and proportionality of the Processing in relation to the Services;

an assessment of the risks to the rights and freedoms of Data Subjects; and

the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller

may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

nature of the data to be protected;

harm that might result from a Personal Data Breach;

state of technological development; and

cost of implementing any measures;

ensure that :

the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));

it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);

are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

have undergone adequate training in the use, care, protection and handling of Personal Data;

not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

the Data Subject has enforceable rights and effective legal remedies;

the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

receives a Data Subject Access Request (or purported Data Subject Access Request);

receives a request to rectify, block or erase any Personal Data;

receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

becomes aware of a Personal Data Breach.

The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

the Controller with full details and copies of the complaint, communication or request;

such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

assistance as requested by the Controller following any Personal Data Breach; and/or

assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

the Controller determines that the Processing is not occasional;

the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

notify the Controller in writing of the intended Subprocessor and Processing;

obtain the written consent of the Controller;

enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

The Relevant Authority may, at any time on not less than 30 Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 30 Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

**Where the Parties are Joint Controllers of Personal Data**

In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (*Processing Data*).

**Independent Controllers of Personal Data**

With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

The Parties shall only provide Personal Data to each other:

to the extent necessary to perform their respective obligations under the Contract;

in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the GDPR); and

where it has recorded it in Annex 1 *(Processing Personal Data).*

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.

A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 GDPR and shall make the record available to the other Party upon reasonable request.

Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has

received the same and shall forward such request or correspondence to the other Party; and

provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

implement any measures necessary to restore the security of any compromised Personal Data;

work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

Notwithstanding the general application of paragraphs 2 to 15 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs16 to 27 of this Joint Schedule 11.

## Annex 1 - Processing Personal Data

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

(a) The contact details of the Relevant Authority's Data Protection Officer are: REDACTED
(b) The contact details of the Supplier's Data Protection Officer: REDACTED, REDACTED
(c) The Processor shall comply with any further written instructions with respect to Processing by the Controller.
(d) Any such further instructions shall be incorporated into this Annex.

| Description | Details |
|---|---|
| Identity of Controller for each Category of Personal Data | **The Supplier is Controller and the Relevant Authority is Processor**<br><br>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data:<br><br>Health Assured is the Controller for all files, notes, records, transcripts and other data collated or generated during the course of providing the services.<br><br>Health Assured are responsible for determining what data is collated and how it is processed for the purposes of providing the requested services -similarly, we would be unable to share service user counselling data or amend or delete it at the client (their employer)'s request.<br><br>This is reflected in all of Health Assured's contractual relationships, and Health Assured are committed to ensuring that they are maintaining the confidentiality and privacy of our service user's data. |
| Duration of the Processing | The processing will take place for the duration of the contract and any extensions to the contract. |
| Nature and purposes of the Processing | The nature of processing of the IPO and Supplier details will include the storage and use of names and business or personal contact details of staff of both the IPO and the Supplier as necessary to deliver the Services and to undertake the Contract and provide support services |

| | |
|---|---|
| | The Contract itself will include the names and business contact details of staff of both the IPO and the Supplier involved in managing the Contract. |
| Type of Personal Data | Names, telephone numbers and email addresses of consulted stakeholders and IPO staff as necessary to deliver the Services. Names, business (&/or personal) telephone numbers and email addresses, office location and position of staff of both the IPO and the Supplier as necessary to deliver the Services and to undertake Contract and performance management.<br><br>The Contract itself will include the names and business contact details of staff of both the IPO and the Supplier involved in managing the Contract |
| Categories of Data Subject | Stakeholders consulted during the period of the contract. Staff of the IPO and the Supplier, including where those employees are named within the Contract itself, use the services offered by the supplier or involved within contract management |
| Plan for return and destruction of the data once the Processing is complete<br><br>UNLESS requirement under Union or Member State law to preserve that type of data | According to IPO disposal & retention policies.<br><br>Health Assured Ltd: All data will be stored securely; electronic records via individual password restricted access to computer systems, and physical or non-electronic records in locked filing systems with access only by authorised persons. No data will be stored for longer than is necessary, data which is no longer required will be securely destroyed, subject to the Health Assured Ltd Retention Policy: Health Assured retain such data in line with our retention policy for a period of 7 years from the termination date of the client's services agreement. This is to cover the 6 years under the Limitations Act plus the current year, when the personal data will be securely deleted |

## Annex 2 - Joint Controller Agreement

### 1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 of Joint Schedule 11

(Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Relevant Authority]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

11.1.2 **Undertakings of both Parties**

(a) The Supplier and the Relevant Authority each undertake that they shall:

(a) report to the other Party every [x] months on:

(i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:

(i) nature of the data to be protected;

(i) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3**. Data Protection Breach**

3.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the Relevant Authority and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

(b) all reasonable assistance, including:

(A) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(B) co-operation with the other Party including taking such reasonable steps as are directed by the Relevant Authority to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(C) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(D) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4**. Audit**

4.1 The Supplier shall permit:

. the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy

and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

d) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

**5. Impact Assessments**

5.1 The Parties shall:

. provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

e) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 GDPR.

**6. ICO Guidance**

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

**7. Liabilities for Data Protection Breach**

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction

of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

- if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

- if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (*Resolving disputes*).

7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("**Court**") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "**Claim Losses**"):

. if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;

- if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

- if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

**8. Termination**

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

**9. Sub-Processing**

10.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

**10. Data Retention**

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.