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

# Order Form Template

, London, EC2M 1QS

|  |  |  |
| --- | --- | --- |
| CALL-OFF REFERENCE: | | 1.11.4.4549. |
|  |  |
| THE BUYER: |  | The Health and Safety Executive |
| BUYER ADDRESS |  | Redgrave Court, Merton Road, Bootle, L20 7HS |
| THE SUPPLIER: |  | Unify Holding UK 1 Limited |
| SUPPLIER ADDRESS: |  | 12th Floor, Dashwood House, 69 Old Broad Street, |

DUNS NUMBER: 230557517

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

If an electronic purchasing system is used instead of signing as a hard-copy, text below must be copied into the electronic order form **starting from ‘APPLICABLE FRAMEWORK CONTRACT’ and up to, but not including, the** **Signature block**

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 30th October 2024.

It’s issued under the Framework Contract with the reference number RM6116 for the provision of HSE’s Contact Centre and Enterprise Telephony requirements.

CALL-OFF LOT(S):

## Lot 4b: Digital Communication Services (Unified Communications)

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) RM6116 3. The following Schedules in equal order of precedence:

* + Joint Schedules for RM6116 o Joint Schedule 2 (Variation Form) o Joint Schedule 3 (Insurance Requirements) o Joint Schedule 4 (Commercially Sensitive Information)
    - Joint Schedule 6 (Key Subcontractors) o Joint Schedule 7 (Financial Difficulties)

Joint Schedule 8 (Guarantee) (Not used)

o Joint Schedule 10 (Rectification Plan)

* + - Joint Schedule 11 (Processing Data)
    - Joint Schedule 12 (Supply Chain Visibility)

* + Call-Off Schedules for RM6116
    - Call-Off Schedule 2 (Staff Transfer) (Not used)

o Call-Off Schedule 3 (Continuous Improvement)

* + - Call-Off Schedule 5 (Pricing Details) o Call-Off Schedule 6 (ICT Services) o Call-Off Schedule 7 (Key Supplier Staff) o Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
    - Call-Off Schedule 9 (Security) o Call-Off Schedule 10 (Exit Management) o Call-Off Schedule 11 (Installation Works) o Call-Off Schedule 13 (Implementation Plan and Testing) o Call-Off Schedule 14 (Service Levels) o Call-Off Schedule 15 (Call-Off Contract Management) o Call-Off Schedule 18 (Background Checks)
    - Call-Off Schedule 20 (Call-Off Specification) o CCS Core Terms (version 3.0.11)

1. Joint Schedule 5 (Corporate Social Responsibility) RM6116
2. 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.
3. Call-Off schedule 25 (Supplier Operational Terms) (Not used)

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 START DATE: |  | **30th October 2024** |
| CALL-OFF EXPIRY DATE: |  | **29th October 2026** |
| CALL-OFF INITIAL PERIOD: |  | **2 years** |

CALL-OFF OPTIONAL EXTENSION PERIOD **2 years in 1 year increments**

MINIMUM PERIOD OF NOTICE FOR WITHOUT REASON TERMINATION

The Buyer may terminate this Call-Off Contract at any time by giving the Supplier not less than 90 days’ prior written notice. In the event the Buyer terminates this Call-Off

Contract prior to the expiry of this Call-Off Initial Period, or any applicable Call-Off Extension Period, the Buyer shall pay the Supplier early Termination Charges in accordance with Framework Special Term 6, (which serves to amend Core Terms Clause 10.3.2 of the Framework Contract).

CALL-OFF DELIVERABLES VIA FURTHER COMPETITION

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 £457,302.00.

CALL-OFF CHARGES

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

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

BACS

All invoices raised must include the relevant Purchase Order number which will be issued by HSE Procurement Unit, each invoice must refer to and state items as listed on the Purchase Order. Failure to include the Purchase Order Number may delay payment. Invoices should be submitted electronically in PDF format to HSE shall make payment of agreed costs, in arrears, within 30 days of the acceptance of the invoice. The Contractor shall send a copy invoice along with details of any work satisfactory carried out to the HSE Contract Manager below.

BUYER’S INVOICE ADDRESS:

Newport SSCL - Health & Safety Executive

PO Box 401

Newport

NP10 8FZ

Email:

BUYER’S AUTHORISED REPRESENTATIVE

BUYER’S SECURITY POLICY

[Security policies (hse.int)](http://intranet.hse.int/security/policy.htm)

SUPPLIER’S AUTHORISED REPRESENTATIVE

SUPPLIER’S CONTRACT MANAGER

PROGRESS REPORT FREQUENCY

On the first Working Day of each calendar month

PROGRESS MEETING FREQUENCY

On the first Working Day of each calendar month

KEY STAFF

Review Call-Off Schedule 7 (Key Supplier Staff)

KEY SUBCONTRACTOR(S)

**[N/A**]

COMMERCIALLY SENSITIVE INFORMATION

[Supplier’s Commercially Sensitive Information]

SERVICE CREDITS

As outlined within Annex 4 of the Call-Off Specification.

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

NOT REQUIRED AS PER TENDER

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)]

|  |  |  |  |
| --- | --- | --- | --- |
| **For and on behalf of the Supplier:** | | **For and on behalf of the Buyer:** | |
| Signature: |  | Signature: |  |
| Name: |  | Name: | David Murray |
| Role: | Unify Head of UKISA (UK&Ireland and South  Africa) | Role: | Director of Finance & Corporate Services |
| Date: | 11 /19/2024 | 11:56 AM PST | Date: | 29/11/2024 |

execution by seal / deed where required by the Buyer.

***Incorporated terms and Schedules***

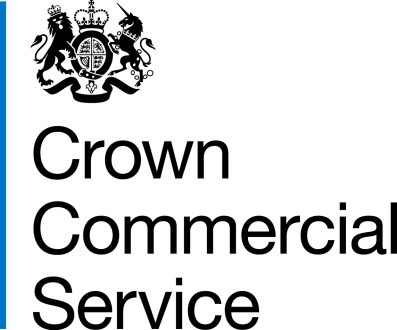
|  |  |
| --- | --- |
| Core Terms | RM6116-NS3-Core-t erms-v3.0.11.docx |
| Joint Schedule 2 | RM6116-Joint-Sched ule-2-Variation-Form- |
| Joint Schedule 3 | RM6116-Joint-Sched ule-3-Insurance-Requ |

|  |  |
| --- | --- |
| Joint Schedule 4  SUPPLIER PLEASE  COMPLETE IF  APPLICABLE – | RM6116-Joint-Sched ule-4-Commercially-S |
| Joint Schedule 5 | RM6116-Joint-Sched ule-5-Corporate-Socia |
| Joint Schedule 6  SUPPLIER PLEASE  COMPLETE IF  APPLICABLE | RM6116-Joint-Sched ule-6-Key-Subcontrac |
| Joint Schedule 7 | RM6116-Joint-Sched ule-7-Financial-Difficu |
| Joint Schedule 8  **NOT REQUIRED** | RM6116-Joint-Sched ule-8-Guarantee-for-P |

|  |  |
| --- | --- |
| Joint Schedule 10 | RM6116-Joint-Sched ule-10-Rectification-P |
| Joint Schedule 11 | RM6116-Joint-Sched ule-11-Processing-Da |
| Joint Schedule 12 | RM6116-Joint-Sched ule-12-Supply-Chain-V |
| Call-Off Schedule 2  **NOT APPLICABLE** | RM6116-Call-Off-Sch  edule-2-Staff-Transfer |
| Call-Off Schedule 3 | RM6116-Call-Off-Sch edule-3-Continuous-Im |
| Call-Off Schedule 4 | RM6116-Call-Off-Sch  edule-4-Call-Off-Tend |

|  |  |
| --- | --- |
| Call-Off Schedule 5 | RM6116-Call-Off-Sch  edule-5-Pricing-Detail |
| Call-Off Schedule 6 | RM6116-Call-Off-Sch  edule-6-ICT-Services-v |
| Call-Off Schedule 7 | RM6116-Call-Off-Sch  edule-7-Key-Supplier- |
| Call-Off Schedule 8 | RM6116-Call-Off-Sch  edule-8-Business-Con |
| Call-Off Schedule 9 | RM6116-Call-Off-Sch  edule-9-Security-vFina |
| Call-Off Schedule 10 | RM6116-Call-Off-Sch edule-10-Exit-Manage |
| Call-Off Schedule 11 | RM6116-Call-Off-Sch  edule-11-Installation- |
| Call-Off Schedule 13 | RM6116-Call-Off-Sch edule-13-Implementa |
| Call-Off Schedule 14  PART B BEING USED – FURTHER INFORMATION  WITHIN SCHEDULE 20 | RM6116-Call-Off-Sch  edule-14-Service-Leve |
| Call-Off Schedule 15 | RM6116-Call-Off-Sch  edule-15-Call-Off-Con |

|  |  |
| --- | --- |
| Call-Off Schedule 18 | RM6116-Call-Off-Sch edule-18-Background |
| Call-Off Schedule 20 | Schedule A  Statement of Services |
| Call-Off Schedule 25  **NOT APPLICABLE** | RM6116-Call-Off-Sch  edule-25-Supplier-Op |



**Core Terms**

**1. Definitions used in the contract**

Interpret this Contract using Joint Schedule 1 (Definitions).

## 2. How the contract works

2.1 The Supplier is eligible for the award of Call-Off Contracts during the Framework Contract Period.

2.2 CCS does not guarantee the Supplier any exclusivity, quantity or value of work under the Framework Contract.

2.3 CCS has paid one penny to the Supplier legally to form the Framework Contract. The Supplier acknowledges this payment.

2.4 If the Buyer decides to buy Deliverables under the Framework Contract it must use Framework Schedule 7 (Call-Off Award Procedure) and must state its requirements using Framework Schedule 6 (Order Form Template and Call-Off Schedules). If allowed by the Regulations, the Buyer can:

1. make changes to Framework Schedule 6 (Order Form Template and Call-Off Schedules);
2. create new Call-Off Schedules;
3. exclude optional template Call-Off Schedules; and/or
4. use Special Terms in the Order Form to add or change terms.

2.5 Each Call-Off Contract:

1. is a separate Contract from the Framework Contract;
2. is between a Supplier and a Buyer;
3. includes Core Terms, Schedules and any other changes or items in the completed Order Form; and (d) survives the termination of the Framework Contract.

* 1. Where the Supplier is approached by any Other Contracting Authority requesting Deliverables or substantially similar goods or services, the Supplier must tell them about this Framework Contract before accepting their order.

* 1. The Supplier acknowledges it has all the information required to perform its obligations under each Contract before entering into a Contract. When information is provided by a Relevant Authority no warranty of its accuracy is given to the Supplier.

* 1. The Supplier will not be excused from any obligation, or be entitled to additional Costs or Charges because it failed to either:

(a) verify the accuracy of the Due Diligence Information; or (b) properly perform its own adequate checks.

2.9 CCS and the Buyer will not be liable for errors, omissions or misrepresentation of any information.

2.10 The Supplier warrants and represents that all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

## 3. What needs to be delivered

### 3.1 All deliverables

3.1.1 The Supplier must provide Deliverables:

1. that comply with the Specification, the Framework Tender Response and, in relation to a Call-Off Contract, the Call-Off Tender (if there is one);
2. to a professional standard;
3. using reasonable skill and care; (d) using Good Industry Practice;

(e) using its own policies, processes and internal quality control measures as long as they do not conflict with the Contract; (f) on the dates agreed; and (g) that comply with Law.

3.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days from Delivery against all obvious defects.

### 3.2 Goods clauses

3.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.

3.2.2 All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.

3.2.3 The Supplier transfers ownership of the Goods on Delivery or payment for those Goods, whichever is earlier.

3.2.4 Risk in the Goods transfers to the Buyer on Delivery of the Goods, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.

3.2.5 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

3.2.6 The Supplier must deliver the Goods on the date and to the specified location during the Buyer’s working hours.

3.2.7 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.

3.2.8 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.

3.2.9 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.

3.2.10 The Supplier must indemnify the Buyer against the costs of any Recall of the Goods and give notice of actual or anticipated action about the Recall of the Goods.

3.2.11 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days notice then it will pay the Supplier’s reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable steps to minimise these costs.

3.2.12 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer’s option and request) any Goods that the Buyer rejects because they do not conform with Clause 3. If the Supplier does not do this it will pay the Buyer’s costs including repair or re-supply by a third party.

### 3.3 Services clauses

3.3.1 Late Delivery of the Services will be a Default of a Call-Off Contract.

3.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the Delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions.

3.3.3 The Supplier must at its own risk and expense provide all Supplier Equipment required to Deliver the Services.

3.3.4 The Supplier must allocate sufficient resources and appropriate expertise to each Contract.

3.3.5 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer’s operations, employees or other contractors.

3.3.6 The Supplier must ensure all Services, and anything used to Deliver the Services, are of good quality and free from defects.

3.3.7 The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

## 4. Pricing and payments

4.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the Charges in the Order Form.

4.2 CCS must invoice the Supplier for the Management Charge and the Supplier must pay it using the process in Framework Schedule 5 (Management Charges and Information).

4.3 All Charges and the Management Charge:

(a) exclude VAT, which is payable on provision of a valid VAT invoice; and (b) include all costs connected with the Supply of Deliverables.

4.4 The Buyer must pay the Supplier the Charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds using the payment method and details stated in the Order Form.

4.5 A Supplier invoice is only valid if it:

1. includes all appropriate references including the Contract reference number and other details reasonably requested by the Buyer;
2. includes a detailed breakdown of Delivered Deliverables and Milestone(s) (if any); and
3. does not include any Management Charge (the Supplier must not charge the Buyer in any way for the Management Charge).

* 1. The Buyer must accept and process for payment an undisputed Electronic Invoice received from the Supplier.

* 1. The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.

* 1. The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this does not happen, CCS or the Buyer can publish the details of the late payment or non-payment.

* 1. If CCS or the Buyer can get more favourable commercial terms for the supply at cost of any materials, goods or services used by the Supplier to provide the Deliverables, then CCS or the Buyer may require the Supplier to replace its existing commercial terms with the more favourable terms offered for the relevant items.

* 1. If CCS or the Buyer uses Clause 4.9 then the Framework Prices (and where applicable, the Charges) must be reduced by an agreed amount by using the Variation Procedure.

* 1. The Supplier has no right of set-off, counterclaim, discount or abatement unless they are ordered to do so by a court.

## 5. The buyer’s obligations to the supplier

5.1 If Supplier Non-Performance arises from an Authority Cause:

1. neither CCS or the Buyer can terminate a Contract under Clause 10.4.1;
2. the Supplier is entitled to reasonable and proven additional expenses and to relief from liability and Deduction under this Contract;
3. the Supplier is entitled to additional time needed to make the Delivery; and
4. the Supplier cannot suspend the ongoing supply of Deliverables.

5.2 Clause 5.1 only applies if the Supplier:

1. gives notice to the Party responsible for the Authority Cause within 10 Working Days of becoming aware;
2. demonstrates that the Supplier Non-Performance would not have occurred but for the Authority

Cause; and

1. mitigated the impact of the Authority Cause.

## 6. Record keeping and reporting

6.1 The Supplier must attend Progress Meetings with the Buyer and provide Progress Reports when specified in the Order Form.

6.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract:

1. during the Contract Period;
2. for 7 years after the End Date; and (c) in accordance with UK GDPR, including but not limited to the records and accounts stated in the definition of Audit in Joint Schedule 1.

* 1. The Relevant Authority or an Auditor can Audit the Supplier.

* 1. During an Audit, the Supplier must:

1. allow the Relevant Authority or any Auditor access to their premises to verify all contract accounts and records of everything to do with the Contract and provide copies for an Audit; and
2. provide information to the Relevant Authority or to the Auditor and reasonable co-operation at their request.

* 1. Where the Audit of the Supplier is carried out by an Auditor, the Auditor shall be entitled to share any information obtained during the Audit with the Relevant Authority.

* 1. If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

1. tell the Relevant Authority and give reasons;
2. propose corrective action; and
3. provide a deadline for completing the corrective action.

6.7 The Supplier must provide CCS with a Self Audit Certificate supported by an audit report at the end of each Contract Year. The report must contain:

1. the methodology of the review;
2. the sampling techniques applied; (c) details of any issues; and (d) any remedial action taken.

6.8 The Self Audit Certificate must be completed and signed by an auditor or senior member of the Supplier’s management team that is qualified in either a relevant audit or financial discipline.

## 7. Supplier staff

7.1 The Supplier Staff involved in the performance of each Contract must:

1. be appropriately trained and qualified;
2. be vetted using Good Industry Practice and the Security Policy; and (c) comply with all conduct requirements when on the Buyer’s Premises.

* 1. Where a Buyer decides one of the Supplier’s Staff is not suitable to work on a contract, the Supplier must replace them with a suitably qualified alternative.

* 1. If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach Clause 27.

* 1. The Supplier must provide a list of Supplier Staff needing to access the Buyer’s Premises and say why access is required.

* 1. The Supplier indemnifies CCS and the Buyer against all claims brought by any person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

## 8. Rights and protection

8.1 The Supplier warrants and represents that:

1. it has full capacity and authority to enter into and to perform each Contract;
2. each Contract is executed by its authorised representative;
3. it is a legally valid and existing organisation incorporated in the place it was formed;
4. there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates that might affect its ability to perform each Contract;
5. it maintains all necessary rights, authorisations, licences and consents to perform its obligations under each Contract;
6. it does not have any contractual obligations which are likely to have a material adverse effect on its ability to perform each Contract;
7. it is not impacted by an Insolvency Event; and (h) it will comply with each Call-Off Contract.

* 1. The warranties and representations in Clauses 2.10 and 8.1 are repeated each time the Supplier provides Deliverables under the Contract.

* 1. The Supplier indemnifies both CCS and every Buyer against each of the following:

(a) wilful misconduct of the Supplier, Subcontractor and Supplier Staff that impacts the Contract; and (b) non-payment by the Supplier of any Tax or National Insurance.

8.4 All claims indemnified under this Contract must use Clause 26.

8.5 The description of any provision of this Contract as a warranty does not prevent CCS or a Buyer from exercising any termination right that it may have for breach of that clause by the Supplier.

8.6 If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify CCS and every Buyer.

8.7 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer’s benefit by the Supplier.

## 9. Intellectual Property Rights (IPRs)

9.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier’s Existing IPR to enable it to both:

1. receive and use the Deliverables; and
2. make use of the deliverables provided by a Replacement Supplier.

* 1. Any New IPR created under a Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs and New IPRs for the purpose of fulfilling its obligations during the Contract Period.

* 1. Where a Party acquires ownership of IPRs incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

* 1. Neither Party has the right to use the other Party’s IPRs, including any use of the other Party’s names, logos or trademarks, except as provided in Clause 9 or otherwise agreed in writing.

* 1. If there is an IPR Claim, the Supplier indemnifies CCS and each Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.

* 1. If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer’s sole option, either:

1. obtain for CCS and the Buyer the rights in Clause 9.1 and 9.2 without infringing any third party IPR; or
2. replace or modify the relevant item with substitutes that do not infringe IPR without adversely affecting the functionality or performance of the Deliverables.

9.7 In spite of any other provisions of a Contract and for the avoidance of doubt, award of a Contract by the Buyer and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949. The Supplier acknowledges that any authorisation by the Buyer under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific IPR involved.

## 10. Ending the contract or any subcontract

### 10.1 Contract Period

10.1.1 The Contract takes effect on the Start Date and ends on the End Date or earlier if required by Law.

10.1.2 The Relevant Authority can extend the Contract for the Extension Period by giving the Supplier no less than 3 Months' written notice before the Contract expires.

### 10.2 Ending the contract without a reason

10.2.1 CCS has the right to terminate the Framework Contract at any time without reason by giving the Supplier at least 30 days' notice.

10.2.2 Each Buyer has the right to terminate their Call-Off Contract at any time without reason by giving the Supplier not less than 90 days' written notice.

### 10.3 Rectification plan process

10.3.1 If there is a Default, the Relevant Authority may, without limiting its other rights, request that the Supplier provide a Rectification Plan, within 10 working days .

10.3.2 When the Relevant Authority receives a requested Rectification Plan it can either:

1. reject the Rectification Plan or revised Rectification Plan, giving reasons; or
2. accept the Rectification Plan or revised Rectification Plan (without limiting its rights) and the Supplier must immediately start work on the actions in the Rectification Plan at its own cost, unless agreed otherwise by the Parties.

10.3.3 Where the Rectification Plan or revised Rectification Plan is rejected, the Relevant Authority:

1. must give reasonable grounds for its decision; and
2. may request that the Supplier provides a revised Rectification Plan within 5 Working Days.

10.3.4 If the Relevant Authority rejects any Rectification Plan, including any revised Rectification Plan, the Relevant Authority does not have to request a revised Rectification Plan before exercising its right to terminate its Contract under Clause 10.4.3(a).

### 10.4 When CCS or the buyer can end a contract

10.4.1 If any of the following events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

1. there is a Supplier Insolvency Event;
2. there is a Default that is not corrected in line with an accepted Rectification Plan;
3. the Supplier does not provide a Rectification Plan within 10 days of the request;
4. there is any material Default of the Contract;
5. there is any material Default of any Joint Controller Agreement relating to any Contract;
6. there is a Default of Clauses 2.10, 9, 14, 15, 27, 32 or Framework Schedule 9 (Cyber Essentials) (where applicable) relating to any Contract;
7. there is a consistent repeated failure to meet the Performance Indicators in Framework Schedule 4 (Framework Management);
8. there is a Change of Control of the Supplier which is not pre-approved by the Relevant Authority in writing;
9. if the Relevant Authority discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded; or
10. the Supplier or its Affiliates embarrass or bring CCS or the Buyer into disrepute or diminish the public trust in them.

10.4.2 CCS may terminate the Framework Contract if a Buyer terminates a Call-Off Contract for any of the reasons listed in Clause 10.4.1.

10.4.3 If any of the following non-fault based events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

1. the Relevant Authority rejects a Rectification Plan;
2. there is a Variation which cannot be agreed using Clause 24 (Changing the contract) or resolved using Clause 34 (Resolving disputes);
3. if there is a declaration of ineffectiveness in respect of any Variation; or (d) the events in 73 (1) (a) of the Regulations happen.

### 10.5 When the supplier can end the contract

The Supplier can issue a Reminder Notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate a Call-Off Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the annual Contract Value within 30 days of the date of the Reminder Notice.

### 10.6 What happens if the contract ends

10.6.1 Where a Party terminates a Contract under any of Clauses 10.2.1, 10.2.2, 10.4.1, 10.4.2, 10.4.3, 10.5 or

20.2 or a Contract expires all of the following apply:

1. The Buyer’s payment obligations under the terminated Contract stop immediately.
2. Accumulated rights of the Parties are not affected.
3. The Supplier must promptly repay to the Buyer any and all Charges the Buyer has paid in advance in respect of Deliverables not provided by the Supplier as at the End Date.
4. The Supplier must promptly delete or return the Government Data except where required to retain copies by Law.
5. The Supplier must promptly return any of CCS or the Buyer’s property provided under the terminated Contract.
6. The Supplier must, at no cost to CCS or the Buyer, co-operate fully in the handover and reprocurement (including to a Replacement Supplier).

10.6.2 In addition to the consequences of termination listed in Clause 10.6.1, where the Relevant Authority terminates a Contract under Clause 10.4.1 the Supplier is also responsible for the Relevant Authority’s reasonable costs of procuring Replacement Deliverables for the rest of the Contract Period.

10.6.3 In addition to the consequences of termination listed in Clause 10.6.1, if either the Relevant Authority terminates a Contract under Clause 10.2.1 or 10.2.2 or a Supplier terminates a Call-Off Contract under Clause 10.5:

1. the Buyer must promptly pay all outstanding Charges incurred to the Supplier; and
2. the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated.

10.6.4 In addition to the consequences of termination listed in Clause 10.6.1, where a Party terminates under Clause 20.2 each Party must cover its own Losses.

10.6.5 The following Clauses survive the termination or expiry of each Contract: 3.2.10, 4.2, 6, 7.5, 9, 11, 12.2, 14, 15, 16, 17, 18, 31.3, 34, 35 and any Clauses and Schedules which are expressly or by implication intended to continue.

### 10.7 Partially ending and suspending the contract

10.7.1 Where CCS has the right to terminate the Framework Contract it can suspend the Supplier's ability to accept Orders (for any period) and the Supplier cannot enter into any new Call-Off Contracts during this period. If this happens, the Supplier must still meet its obligations under any existing Call-Off Contracts that have already been signed.

10.7.2 Where CCS has the right to terminate a Framework Contract it is entitled to terminate all or part of it.

10.7.3 Where the Buyer has the right to terminate a Call-Off Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends a Contract it can provide the Deliverables itself or buy them from a third party.

10.7.4 The Relevant Authority can only partially terminate or suspend a Contract if the remaining parts of that Contract can still be used to effectively deliver the intended purpose.

10.7.5 The Parties must agree any necessary Variation required by Clause 10.7 using the Variation Procedure, but the Supplier may not either:

1. reject the Variation; or
2. increase the Charges, except where the right to partial termination is under Clause 10.2.

10.7.6 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under Clause 10.7.

### 10.8 When subcontracts can be ended

At the Buyer’s request, the Supplier must terminate any Subcontracts in any of the following events:

1. there is a Change of Control of a Subcontractor which is not pre-approved by the Relevant Authority in writing;
2. the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 10.4; or
3. a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Relevant Authority.

## 11. How much you can be held responsible for

11.1 Each Party's total aggregate liability in each Contract Year under this Framework Contract (whether in tort, contract or otherwise) is no more than £1,000,000.

11.2 Each Party's total aggregate liability in each Contract Year under each Call-Off Contract (whether in tort, contract or otherwise) is no more than the greater of £5 million or 150% of the Estimated Yearly Charges unless specified in the Call-Off Order Form.

11.3 No Party is liable to the other for:

1. any indirect Losses; or
2. Loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

11.4 In spite of Clause 11.1 and 11.2, neither Party limits or excludes any of the following:

1. its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors;
2. its liability for bribery or fraud or fraudulent misrepresentation by it or its employees;
3. any liability that cannot be excluded or limited by Law;
4. its obligation to pay the required Management Charge or Default Management Charge.

* 1. In spite of Clauses 11.1 and 11.2, the Supplier does not limit or exclude its liability for any indemnity given under Clauses 7.5, 8.3(b), 9.5, 31.3 or Call-Off Schedule 2 (Staff Transfer) of a Contract.

* 1. In spite of Clauses 11.1, 11.2 but subject to Clauses 11.3 and 11.4, the Supplier's aggregate liability in each and any Contract Year under each Contract under Clause 14.8 shall in no event exceed the Data Protection Liability Cap.

* 1. Each Party must use all reasonable endeavours to mitigate any Loss or damage which it suffers under or in connection with each Contract, including any indemnities.

* 1. When calculating the Supplier’s liability under Clause 11.1 or 11.2 the following items will not be taken into consideration:

1. Deductions; and
2. any items specified in Clauses 11.5 or 11.6.

11.9 If more than one Supplier is party to a Contract, each Supplier Party is jointly and severally liable for their obligations under that Contract.

## 12. Obeying the law

12.1 The Supplier must use reasonable endeavours to comply with the provisions of Joint Schedule 5 (Corporate Social Responsibility).

12.2 To the extent that it arises as a result of a Default by the Supplier, the Supplier indemnifies the Relevant Authority against any fine or penalty incurred by the Relevant Authority pursuant to Law and any costs incurred by the Relevant Authority in defending any proceedings which result in such fine or penalty.

12.3 The Supplier must appoint a Compliance Officer who must be responsible for ensuring that the Supplier complies with Law, Clause 12.1 and Clauses 27 to 32.

## 13. Insurance

The Supplier must, at its own cost, obtain and maintain the Required Insurances in Joint Schedule 3 (Insurance Requirements) and any Additional Insurances in the Order Form.

## 14. Data protection

14.1 The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with Joint Schedule 11 (Processing Data).

14.2 The Supplier must not remove any ownership or security notices in or relating to the Government Data.

14.3 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every 6 Months.

14.4 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the Security Policy and any applicable Security Management Plan.

14.5 If at any time the Supplier suspects or has reason to believe that the Government Data provided under a Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Relevant Authority and immediately suggest remedial action.

14.6 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Relevant Authority may either or both:

1. tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Relevant Authority receives notice, or the Supplier finds out about the issue, whichever is earlier; and/or
2. restore the Government Data itself or using a third party.

* 1. The Supplier must pay each Party’s reasonable costs of complying with Clause 14.6 unless CCS or the Buyer is at fault.

* 1. The Supplier:

1. must provide the Relevant Authority with all Government Data in an agreed open format within 10 Working Days of a written request;
2. must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;
3. must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice;
4. securely erase all Government Data and any copies it holds when asked to do so by CCS or the Buyer unless required by Law to retain it; and
5. indemnifies CCS and each Buyer against any and all Losses incurred if the Supplier breaches Clause 14 and any Data Protection Legislation.

## 15. What you must keep confidential

15.1 Each Party must:

1. keep all Confidential Information it receives confidential and secure;
2. except as expressly set out in the Contract at Clauses 15.2 to 15.4 or elsewhere in the Contract, not disclose, use or exploit the Disclosing Party’s Confidential Information without the Disclosing Party's prior written consent; and
3. immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

15.2 In spite of Clause 15.1, a Party may disclose Confidential Information which it receives from the Disclosing Party in any of the following instances:

1. where disclosure is required by applicable Law or by a court with the relevant jurisdiction if, to the extent not prohibited by Law, the Recipient Party notifies the Disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;
2. if the Recipient Party already had the information without obligation of confidentiality before it was disclosed by the Disclosing Party;
3. if the information was given to it by a third party without obligation of confidentiality;
4. if the information was in the public domain at the time of the disclosure;
5. if the information was independently developed without access to the Disclosing Party’s Confidential Information;
6. on a confidential basis, to its auditors;
7. on a confidential basis, to its professional advisers on a need-to-know basis; or
8. to the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

* 1. In spite of Clause 15.1, the Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier Staff must enter into a direct confidentiality agreement with the Relevant Authority at its request.

* 1. In spite of Clause 15.1, CCS or the Buyer may disclose Confidential Information in any of the following cases:

1. on a confidential basis to the employees, agents, consultants and contractors of CCS or the Buyer;
2. on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that CCS or the Buyer transfers or proposes to transfer all or any part of its business to;
3. if CCS or the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;
4. where requested by Parliament; or (e) under Clauses 4.7 and 16.

* 1. For the purposes of Clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in Clause 15.

* 1. Transparency Information is not Confidential Information.

* 1. The Supplier must not make any press announcement or publicise the Contracts or any part of them in any way, without the prior written consent of the Relevant Authority and must take all reasonable steps to ensure that Supplier Staff do not either.

## 16. When you can share information

16.1 The Supplier must tell the Relevant Authority within 48 hours if it receives a Request For Information.

16.2 Within five (5) Working Days of the Buyer’s request the Supplier must give CCS and each Buyer full cooperation and information needed so the Buyer can:

1. publish the Transparency Information;
2. comply with any Freedom of Information Act (FOIA) request; and/or
3. comply with any Environmental Information Regulations (EIR) request.

16.3 The Relevant Authority may talk to the Supplier to help it decide whether to publish information under Clause 16. However, the extent, content and format of the disclosure is the Relevant Authority’s decision in its absolute discretion.

## 17. Invalid parts of the contract

If any part of a Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Contract as much as required and rendered ineffective as far as possible without affecting the rest of the Contract, whether it is valid or enforceable.

## 18. No other terms apply

The provisions incorporated into each Contract are the entire agreement between the Parties. The Contract replaces all previous statements, agreements and any course of dealings made between the Parties, whether written or oral, in relation to its subject matter. No other provisions apply.

## 19. Other people’s rights in a contract

No third parties may use the Contracts (Rights of Third Parties) Act 1999 (CRTPA) to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

## 20. Circumstances beyond your control

20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under a Contract while the inability to perform continues, if it both:

1. provides a Force Majeure Notice to the other Party; and
2. uses all reasonable measures practical to reduce the impact of the Force Majeure Event.

20.2 Either Party can partially or fully terminate the affected Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.

## 21. Relationships created by the contract

No Contract creates a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

## 22. Giving up contract rights

A partial or full waiver or relaxation of the terms of a Contract is only valid if it is stated to be a waiver in writing to the other Party.

## 23. Transferring responsibilities

23.1 The Supplier cannot assign, novate or transfer a Contract or any part of a Contract without the Relevant Authority’s written consent.

23.2 The Relevant Authority can assign, novate or transfer its Contract or any part of it to any Central

Government Body, public or private sector body which performs the functions of the Relevant Authority.

23.3 When CCS or the Buyer uses its rights under Clause 23.2 the Supplier must enter into a novation agreement in the form that CCS or the Buyer specifies.

23.4 The Supplier can terminate a Contract novated under Clause 23.2 to a private sector body that is experiencing an Insolvency Event.

23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

23.6 If CCS or the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of Subcontractors at all levels of the supply chain including:

1. their name;
2. the scope of their appointment; and (c) the duration of their appointment.

## 24. Changing the contract

24.1 Either Party can request a Variation which is only effective if agreed in writing and signed by both Parties.

24.2 The Supplier must provide an Impact Assessment either:

1. with the Variation Form, where the Supplier requests the Variation; or
2. within the time limits included in a Variation Form requested by CCS or the Buyer.

24.3 If the Variation cannot be agreed or resolved by the Parties, CCS or the Buyer can either:

1. agree that the Contract continues without the Variation; or
2. terminate the affected Contract, unless in the case of a Call-Off Contract, the Supplier has already provided part or all of the provision of the Deliverables, or where the Supplier can show evidence of substantial work being carried out to provide them; or
3. refer the Dispute to be resolved using Clause 34 (Resolving Disputes).

* 1. CCS and the Buyer are not required to accept a Variation request made by the Supplier.

* 1. If there is a General Change in Law, the Supplier must bear the risk of the change and is not entitled to ask for an increase to the Framework Prices or the Charges.

* 1. If there is a Specific Change in Law or one is likely to happen during the Contract Period the Supplier must give CCS and the Buyer notice of the likely effects of the changes as soon as reasonably practical. They must also say if they think any Variation is needed either to the Deliverables, Framework Prices or a Contract and provide evidence:

(a) that the Supplier has kept costs as low as possible, including in Subcontractor costs; and (b) of how it has affected the Supplier’s costs.

24.7 Any change in the Framework Prices or relief from the Supplier's obligations because of a Specific Change in Law must be implemented using Clauses 24.1 to 24.4.

24.8 For 101(5) of the Regulations, if the Court declares any Variation ineffective, the Parties agree that their mutual rights and obligations will be regulated by the terms of the Contract as they existed immediately prior to that Variation and as if the Parties had never entered into that Variation.

## 25. How to communicate about the contract

25.1 All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they are delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective at 9:00am on the first Working Day after sending unless an error message is received.

25.2 Notices to CCS must be sent to the CCS Authorised Representative’s address or email address in the Framework Award Form.

25.3 Notices to the Buyer must be sent to the Buyer Authorised Representative’s address or email address in the Order Form.

25.4 This Clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

## 26. Dealing with claims

26.1 If a Beneficiary is notified of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days.

26.2 At the Indemnifier’s cost the Beneficiary must both:

(a) allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim; and (b) give the Indemnifier reasonable assistance with the claim if requested.

26.3 The Beneficiary must not make admissions about the Claim without the prior written consent of the Indemnifier which can not be unreasonably withheld or delayed.

26.4 The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that does not damage the Beneficiary’s reputation.

26.5 The Indemnifier must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

26.6 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.

26.7 If the Indemnifier pays the Beneficiary money under an indemnity and the Beneficiary later recovers money which is directly related to the Claim, the Beneficiary must immediately repay the Indemnifier the lesser of either:

1. the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money; or
2. the amount the Indemnifier paid the Beneficiary for the Claim.

## 27. Preventing fraud, bribery and corruption

27.1 The Supplier must not during any Contract Period:

1. commit a Prohibited Act or any other criminal offence in the Regulations 57(1) and 57(2); or
2. do or allow anything which would cause CCS or the Buyer, including any of their employees, consultants, contractors, Subcontractors or agents to breach any of the Relevant Requirements or incur any liability under them.

27.2 The Supplier must during the Contract Period:

1. create, maintain and enforce adequate policies and procedures to ensure it complies with the Relevant Requirements to prevent a Prohibited Act and require its Subcontractors to do the same;
2. keep full records to show it has complied with its obligations under Clause 27 and give copies to CCS or the Buyer on request; and
3. if required by the Relevant Authority, within 20 Working Days of the Start Date of the relevant Contract, and then annually, certify in writing to the Relevant Authority, that they have complied with Clause 27, including compliance of Supplier Staff, and provide reasonable supporting evidence of this on request, including its policies and procedures.

27.3 The Supplier must immediately notify CCS and the Buyer if it becomes aware of any breach of Clauses

27.1 or 27.2 or has any reason to think that it, or any of the Supplier Staff, has either:

1. been investigated or prosecuted for an alleged Prohibited Act;
2. been debarred, suspended, proposed for suspension or debarment, or is otherwise ineligible to take part in procurement programmes or contracts because of a Prohibited Act by any government department or agency;
3. received a request or demand for any undue financial or other advantage of any kind related to a Contract; or
4. suspected that any person or Party directly or indirectly related to a Contract has committed or attempted to commit a Prohibited Act.

* 1. If the Supplier notifies CCS or the Buyer as required by Clause 27.3, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

* 1. In any notice the Supplier gives under Clause 27.3 it must specify the:

1. Prohibited Act;
2. identity of the Party who it thinks has committed the Prohibited Act; and
3. action it has decided to take.

## 28. Equality, diversity and human rights

28.1 The Supplier must follow all applicable equality Law when they perform their obligations under the Contract, including:

1. protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and
2. any other requirements and instructions which CCS or the Buyer reasonably imposes related to equality Law.

28.2 The Supplier must take all necessary steps, and inform CCS or the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on a Contract.

## 29. Health and safety

29.1 The Supplier must perform its obligations meeting the requirements of:

1. all applicable Law regarding health and safety; and
2. the Buyer’s current health and safety policy while at the Buyer’s Premises, as provided to the Supplier.

29.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they are aware of at the Buyer Premises that relate to the performance of a Contract.

## 30. Environment

30.1 When working on Site the Supplier must perform its obligations under the Buyer’s current Environmental Policy, which the Buyer must provide.

30.2 The Supplier must ensure that Supplier Staff are aware of the Buyer’s Environmental Policy.

## 31. Tax

31.1 The Supplier must not breach any Tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. CCS and the Buyer cannot terminate a Contract where the Supplier has not paid a minor Tax or social security contribution.

31.2 Where the Charges payable under a Contract with the Buyer are or are likely to exceed £5 million at any point during the relevant Contract Period, and an Occasion of Tax Non-Compliance occurs, the Supplier must notify CCS and the Buyer of it within 5 Working Days including:

1. the steps that the Supplier is taking to address the Occasion of Tax Non-Compliance and any mitigating factors that it considers relevant; and
2. other information relating to the Occasion of Tax Non-Compliance that CCS and the Buyer may reasonably need.

31.3 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under a Call-Off Contract, the Supplier must both:

1. comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions; and
2. indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Contract Period in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

31.4 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains the following requirements:

1. the Buyer may, at any time during the Contract Period, request that the Worker provides information which demonstrates they comply with Clause 31.3, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;
2. the Worker’s contract may be terminated at the Buyer’s request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;
3. the Worker’s contract may be terminated at the Buyer’s request if the Worker provides information which the Buyer considers is not good enough to demonstrate how it complies with Clause 31.3 or confirms that the Worker is not complying with those requirements; and
4. the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.

## 32. Conflict of interest

32.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential Conflict of Interest.

32.2 The Supplier must promptly notify and provide details to CCS and each Buyer if a Conflict of Interest happens or is expected to happen.

32.3 CCS and each Buyer can terminate its Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential Conflict of Interest.

## 33. Reporting a breach of the contract

33.1 As soon as it is aware of it the Supplier and Supplier Staff must report to CCS or the Buyer any actual or suspected breach of:

1. Law;
2. Clause 12.1; or
3. Clauses 27 to 32.

33.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in Clause 33.1 to the Buyer or a Prescribed Person.

## 34. Resolving disputes

34.1 If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

34.2 If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the

Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the

Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using Clauses 34.3 to 34.5.

34.3 Unless the Relevant Authority refers the Dispute to arbitration using Clause 34.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

1. determine the Dispute;
2. grant interim remedies; and/or
3. grant any other provisional or protective relief.

* 1. The Supplier agrees that the Relevant Authority has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

* 1. The Relevant Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under Clause 34.3, unless the Relevant Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under Clause 34.4.

* 1. The Supplier cannot suspend the performance of a Contract during any Dispute.

**35. Which law applies**

This Contract and any Disputes arising out of, or connected to it, are governed by English law.

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

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

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

Signature

Date

Name (in Capitals)

Address

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

Signature

Date

Name (in Capitals)

Address

Framework Ref: RM

Project Version: v1.0

Model Version: v3.0

# Joint Schedule 3 (Insurance Requirements)

## 1. The insurance you need to have

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

1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

1.2.4 maintained for at least six (6) years after the End Date.

1.3 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.

## 2. How to manage the insurance

2.1 Without limiting the other provisions of this Contract, the Supplier shall:

2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

## 3. What happens if you aren’t insured

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

## 4. Evidence of insurance you must provide

4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

## 5. Making sure you are insured to the required amount

5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

## 6. Cancelled Insurance

6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or nonrenewal of any of the Insurances.

6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

## 7. Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.

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

7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

## ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following [standard] insurance cover from the Framework Start Date in accordance with this Schedule:
   1. professional indemnity insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than] one million pounds (£1,000,000);
   2. public liability insurance [with cover (for a single event or a series of related events and in the aggregate)] of not less than one million pounds (£1,000,000); and
   3. employers’ liability insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than] five million pounds (£5,000,000).
   4. product liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000)

Joint Schedule 4 (Commercially Sensitive Information) Crown Copyright 2018

# Joint Schedule 4 (Commercially Sensitive Information)

1. **What is the Commercially Sensitive Information?** 
   1. In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
   2. Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
   3. Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 of the Core Terms (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. | Contract start date | Pricing | Contract duration + 3 years |
| 2. | Contract start date | Supplier Technology including components used in the services | Contract duration + 3 years |

Framework Ref: RM6116

Project Version: v1.0 1

Joint Schedule 4 (Commercially Sensitive Information) Crown Copyright 2018

Framework Ref: RM6116

Project Version: v1.0 2

# Joint Schedule 5 (Corporate Social Responsibility) Part A

## 1. Definitions

|  |  |
| --- | --- |
| **“Corporate Social**  **Responsibility**  **Reports”** | written reports which the Supplier must complete and provide to the Buyer in accordance with Part B of this Schedule; |
| **“Carbon Reduction**  **Plan”** | a plan which contains the details of emissions across a single year against a range of emissions sources and greenhouse gases, as per PPN 06/21; |
| **“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; |
| **“Prohibited Items”** | means those items set out in Table A which the Supplier must not use in its performance of the Contract; and |
| **“Waste Hierarchy”** | means prioritisation of waste management in the following order of preference:  prevention – by using less material in design and manufacture. Keeping products for longer;  preparing for re-use – by checking, cleaning, repairing, refurbishing, whole items or spare parts;  recycling – by turning waste into a new substance or produce, including composting if it meets quality protocols;  other recovery – through anaerobic digestion, incineration with energy recovery, gasification and pyrolysis which produce energy (fuels, heat and power) and materials from waste; some backfilling; and  disposal - Landfill and incineration without energy recovery. |

## 1. What we expect from our Suppliers

1.1 In February 2019, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government.

[(*https://assets.publishing.service.gov.uk/government/uploads/system/upload s/attachment\_data/file/779660/20190220-Supplier\_Code\_of\_Conduct.pdf*)](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779660/20190220-Supplier_Code_of_Conduct.pdf)

1.2 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.

1.3 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.

## 2. Equality and Accessibility

2.1 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:

2.1.1 eliminate discrimination, harassment or victimisation of any kind; and

2.1.2 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.

## 3. Modern Slavery, Child Labour and Inhumane Treatment

3.1 The Supplier:

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

3.1.2 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;

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

3.1.4 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.

3.1.5 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.

3.1.6 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;

3.1.7 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;

3.1.8 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;

3.1.9 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;

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

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

## 4. Income Security

4.1 The Supplier shall:

4.1.1 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;

4.1.2 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;

4.1.3 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;

4.1.4 record all disciplinary measures taken against Supplier Staff; and

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

## 5. Working Hours

5.1 The Supplier shall:

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

5.1.2 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;

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

1. the extent;
2. frequency; and
3. hours worked;

by individuals and by the Supplier Staff as a whole;

* 1. The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.
  2. Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:
     1. this is allowed by national law;
     2. this is allowed by a collective agreement freely negotiated with a workers’ organisation representing a significant portion of the workforce
     3. appropriate safeguards are taken to protect the workers’ health and safety; and
     4. the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

5.4 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.

## 6. Environmental Requirements

6.1. The Supplier shall comply in all material respects with all applicable environmental laws, permits and regulations in force in relation to the Contract.

6.2. The Supplier warrants that it has complied with the principles of ISO 14001 standards throughout the Term.

6.3. The Supplier shall meet the Government Buying Standards applicable to the Deliverables which can be found online at: [https://www.gov.uk/government/collections/sustainable-procurement-thegovernment-buying-standards-gbs.](https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs)

# Part B – Sustainability and Reporting

## 1. Sustainability Requirements

1.1 The Supplier shall complete the Corporate Social Responsibility Report at Paragraph 3 of this Part B in relation to its provision of the Deliverables under this Contract and provide the Corporate Social Responsibility Report to the Buyer on the date and frequency outlined in Table A of this Part B.

1.2 The Supplier shall use reasonable endeavours to avoid the use of paper and card in carrying out its obligations under this Contract. Where unavoidable under reasonable endeavours, the Supplier shall ensure that any paper or card deployed in the performance of the Services consists of one hundred percent (100%) recycled content and used on both sides where feasible to do so.

1.3 The Supplier shall complete and provide CCS with a Carbon Reduction Plan.

1.4 The Supplier shall progress towards carbon net zero during the lifetime of the framework.

## 2. Social Value Requirements

2.1 The Supplier shall complete the Corporate Social Responsibility Report at Paragraph 3 of this Part B in relation its performance on meeting any Social

Value obligations agreed to for the provision of the Deliverables under this Contract and provide the Corporate Social Responsibility Report to the Buyer on the date and frequency outlined in Table A of this Part B.

2.2 The Supplier shall use its best endeavours, as an organisation, to deliver environmental sustainability and protection in the provision of the Deliverables by establishing and delivering against credible targets for delivering energy efficiency throughout the lifetime of the framework.

2.3 The Supplier shall use its best endeavours, as an organisation, to address inequality in employment, skills and pay by supporting disadvantaged, underrepresented and minority groups into employment throughout the lifetime of the framework.

2.4 The Supplier shall use its best endeavours, as an organisation, to promote new opportunities and engage with new and small organisations (e.g. SMEs and VCSEs), to help them grow, supporting their development throughout the lifetime of the framework.

## 3. Reporting Requirements

3.1 The Supplier shall complete the Corporate Social Responsibility Report in relation to its provision of the Deliverables under this Contract and provide the Corporate Social Responsibility Report to the Buyer on the date and frequency outlined in Table A of this Part B.

3.2 The Supplier shall provide the baseline data contained within table B(1) – Baseline data to facilitate subsequent measurement throughout the lifetime of the framework. The information required to populate table B(1) and annually thereafter will be provided to CCS within 10 calendar days of the submission of a request by CCS.

3.3 The Supplier shall complete the Framework Performance Indicator Submission Form at the frequency outlined in Table B of this Part B and return to CCS. The Supplier shall include in the Framework Performance Indicator Submission Form the content specified within Table B.

3.4 The Supplier shall attend Supplier Relationship Meetings with CCS at such times and frequencies as CCS determines from time to time to discuss the information contained in the Framework Performance Indicator Submission Forms. The information will be used to measure progress of social value activity.

3.5 In the event CCS develops an alternative social value measurement tool during the lifetime of the framework, the Performance Indicator measures described at Table B will be superseded by that tool.

## Table A

|  |  |  |  |
| --- | --- | --- | --- |
| Report Name | Content of Report | | Frequency of  Report |
| [Sustainability] | 1. the key sustainability impacts identified; 2. sustainability improvements made; 3. actions underway or planned to reduce sustainability impacts; 4. contributions made to the Buyer’s sustainability policies and   objectives;   1. sustainability policies, standards, targets and practices that have been adopted to reduce the environmental impact of the   Supplier’s operations and evidence of these being actively pursued, indicating arrangements for engagement and achievements. This can also include where positive sustainability impacts have been delivered; and   1. risks to the Service and   Subcontractors of climate change and severe weather events such as flooding and extreme temperatures including mitigation, adaptation and continuity plans employed by the Supplier in response to those risks. | | [On the  [anniversary]of the  Effective Date] |
| [Greenhouse Gas  Emissions] | Indicate greenhouse gas emissions making use of the use of the most recent conversion guidance set out in  'Greenhouse gas reporting – Conversion factors’ available online at  https://www.gov.uk/guidance/measuring -and-reporting-environmental-impactsguidance-for-businesses | | [On the anniversary of the  Effective Date] |
| Water Use | Volume in metres cubed. | | On the anniversary of the Effective Date |
| Energy Use | Separ for:  a.  b.  c.  d.  Power  ac 50600- | ate energy consumption figures assets deployed on the Supplier’s  site; assets deployed on the Authority’s  site; assets deployed off-site; and energy consumed by IT assets and by any cooling devices deployed.  Usage Effectiveness (PUE) rating for each data centre/server room in cordance with ISO/IEC 31034-2/EN  4-2. | On the anniversary of the  Effective Date |
| Social Value | [**Guidance:** Include any relevant Social  Value requirements from the Specification] | | On the anniversary of the  Effective Date |

**Table B** – Submission to CCS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Report Name | Content of Report | Frequency Report |  | of |
| Framework  Performance  Indicator  Submission Form – | MSAT completion and progress recorded against the following 6 areas:   * Governance * Policies and Procedures | Annually |  |  |

|  |  |  |
| --- | --- | --- |
| Modern Slavery  section | * Risk Assessment and   Management   * Due Diligence * Training ● KPI |  |
| Framework  Performance  Indicator  Submission Form –  Carbon Net Zero | The Supplier to demonstrate progression towards carbon net zero by reporting on the below areas     * Number of carbon reduction activities that your organisation has taken to progress your carbon reduction plan * Number of RM6116 carbon reduction activities that benefit the Buyer * List the top 3 carbon reduction activities completed for non   RM6116 contracts | Annually |
| Framework  Performance  Indicator  Submission Form –  Apprenticeships | Supplier shall submit data demonstrating how they are progressing  apprenticeships within their organisation   * Number of apprenticeships started * Cumulative number of apprenticeships ongoing * Number of apprenticeships concluded * Number of apprenticeships retained | Annually |
| Framework  Performance  Indicator  Submission Form –  Diversity &  Inclusion | To demonstrate that suppliers are redressing workforce imbalance within their organisation   * Representation of women * Representation of ethnic minorities * Representation of staff who identify as having a disability * Representation of prison leavers * Representation of LBTQIA+ | Annually |
| Framework  Performance  Indicator  Submission Form – SMEs/VCSEs | To demonstrate that Suppliers are engaging with and developing SMEs/VCSES   * Number of SMEs/VCSES within your supply chain for RM6116 * Number of SME/VCSEs within your supply chain delivering services on RM6116 contracts * How many sub-contract opportunities have there been within the reporting period * Of the sub-contract opportunities, how many were awarded to a   SMEs | Annually |

Table B(1) – Baseline data

|  |  |  |
| --- | --- | --- |
| Report Name | Content of Report | Frequency of Report |
| Apprenticeships baseline data | The Supplier shall submit data demonstrating:     * % of apprentices in their current workforce * % conversion rate of apprentices retained when an   apprenticeship concludes | To be provided to CCS within 10 calendar days of the submission of a request and annually thereafter |
| Diversity of Workforce baseline data | The Supplier shall submit baseline figures of their current UK workforce:     * Representation of women * Representation of ethnic minorities * Representation of staff who identify as having a disability | To be provided to CCS within 10 calendar days of the submission of a request and annually thereafter |

|  |  |  |
| --- | --- | --- |
|  | * Representation of prison leavers * Representation of LBTQIA+ |  |
| SMEs/VCSEs  baseline data | The Supplier shall produce and submit a SME / VCSE engagement strategy detailing how they intend to retain and develop SMEs/VCSEs within their supply chain. | To be provided to CCS within 10 calendar days of the submission of a request and annually thereafter |

**Joint Schedule 6 (Key Subcontractors)** Crown Copyright 2018

## Joint Schedule 6 (Key Subcontractors)

### 1. Restrictions on certain subcontractors

1.1 The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.

1.2 The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.

1.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to section 21 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to the Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;

1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or

1.3.3 the proposed Key Subcontractor employs unfit persons.

1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:

1.4.1 the proposed Key Subcontractor’s name, registered office and company registration number;

1.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;

1.4.3 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm’s-length" terms;

1.4.4 for CCS, the Key Sub-Contract price expressed as a percentage of the total projected Framework Price over the Framework Contract Period;

1.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and

1.4.6 (where applicable) Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.

Framework Ref: RM6116

Project Version: v1.0 1

Model Version: v3.1

**Joint Schedule 6 (Key Subcontractors)**

Crown Copyright 2018

1.5 If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:

1.5.1 a copy of the proposed Key Sub-Contract; and

1.5.2 any further information reasonably requested by CCS and/or the Buyer.

1.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:

1.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;

1.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;

1.6.3 a provision enabling CCS and the Buyer to enforce the Key SubContract as if it were the Supplier;

1.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key SubContract to CCS and/or the Buyer;

1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:

1. the data protection requirements set out in Clause 14 of the

Core Terms (Data protection);

1. the FOIA and other access request requirements set out in Clause 16 of the Core Terms (When you can share information);
2. the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;
3. the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and
4. the conduct of audits set out in Clause 6 of the Core Terms

(Record keeping and reporting);

1.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 of the Core Terms (When CCS or the Buyer can end this contract) and 10.5 of the Core Terms (What happens if the contract ends) of this Contract; and

1.6.7 a provision restricting the ability of the Key Subcontractor to subcontract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

Framework Ref: RM6116

Project Version: v1.0 2

Model Version: v3.1

## Joint Schedule 7 (Financial Difficulties)

**[Guidance: This Schedule provides CCS and the Buyer with the option of using**

**Credit Ratings and/or Financial Indicators for the purposes of the Financial Distress Provisions. Buyers may use any combination of these indicators to suit their own requirements and may delete or amend as required. Buyers should ensure that the drafting of any Financial Indicators aligns with the financial standing criteria used during the selection stage of the procurement]**

### 1. Definitions

1.1 In this Schedule, the following definitions shall apply:

**“Applicable Financial** means the financial indicators from Paragraph 5.1 of

**Indicators”** this Schedule which are to apply to the Monitored Suppliers as set out in Paragraph 5.2 of this Schedule;

**“Board”**  means the Supplier’s board of directors;

**“Board Confirmation”**  means written confirmation from the Board in

accordance with Paragraph 8 of this Schedule;

|  |  |
| --- | --- |
| **“Bronze Contract”** | Call-Off Contract categorised as a Bronze contract using the Cabinet Office Contract Tiering Tool; |
| **“Cabinet Office Markets and**  **Suppliers**  **Team”** | means the UK Government’s team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function; |
| **“Credit Rating Threshold”** | the minimum credit rating level for each entity in the FDE Group as set out in Annex 1 to this Schedule; |
| **“FDE Group”** | means the [Supplier, Key Sub-contractors, [the  Guarantor] and the [Monitored Suppliers]]; |
| **“Financial Distress Event”** | Any of the events listed in Paragraph 3.1 of this Schedule; |

**“Financial Distress**  plan setting out how the Supplier will ensure the **Remediation** continued performance and delivery of the

**Plan”** Deliverables in accordance with the Contract in

the event that a Financial Distress Event occurs;

**“Financial Indicators”** respect of the Supplier, Key Sub-contractors and the Guarantor, means each of the financial indicators set out at paragraph 5.1 of this Schedule and in respect of each Monitored

Supplier, means those Applicable Financial Indicators;

**F “Financial Target**  means the target thresholds for each of the Financial

**Thresholds”** Indicators set out at paragraph 5.1 of this Schedule;

**“Monitored Suppliers”**  means those entities specified at paragraph 5.2 of this Schedule;

**“Rating Agencies”**  the rating agencies listed in Annex 1 of this Schedule;

**“Strategic Supplier”**  means those suppliers to the government listed at [https://www.gov.uk/government/publications/str ategic-suppliers.](https://www.gov.uk/government/publications/strategic-suppliers)

### 2. Warranties and duty to notify

2.1 The Supplier warrants and represents to the Relevant Authority for the benefit of the Relevant Authority that as at the Effective Date:

2.1.1 the long term credit ratings issued for each entity in the FDE

Groupby each of the Rating Agencies are as set out in Annex 2 to this Schedule and;

2.1.2 the financial position or, as appropriate, the financial performance of each Supplier, Guarantor and Key-

Subcontractors satisfies the Financial Target Thresholds.

2.2 The Supplier shall promptly (or shall procure that its auditors promptly notify) the Relevant Authority in writing if there is any downgrade in the credit rating issued by any Rating Agency for any entity in the FDE Group (and in any event within five (5) Working Days of the occurrence of the downgrade).

2.3 The Supplier shall:

2.3.1 regularly monitor the credit ratings of each entity in the FDE Group with the Rating Agencies;

2.3.2 monitor and report on the Financial Indicators for each entity in the FDE Group against the Financial Target Thresholds at least at the frequency set out for each at Paragraph 5.1 (where specified) and in any event, on a regular basis and no less than once a year within ninety (90) days after the Accounting Reference Date; and

2.3.3 promptly notify (or shall procure that its auditors promptly notify) the Relevant Authorityin writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event (and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event).

2.4 For the purposes of determining whether a Financial Distress Event has occurred, pursuant to the provisions of Paragraph 3.1 and for the purposes of determining relief under Paragraph 7.1, the credit rating of an FDE Group entity shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated that entity at or below the applicable Credit Rating Threshold.

### 3. Financial Distress events

3.1 The following shall be Financial Distress Events:

3.1.1 the credit rating of an FDE Group entity dropping below the applicable Credit Rating Threshold;

3.1.2 an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;

3.1.3 there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;

3.1.4 an FDE Group entity committing a material breach of covenant to its lenders;

3.1.5 a Key Sub-contractor notifying CCS or the Buyer that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;

3.1.6 any of the following:

1. commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;
2. non-payment by an FDE Group entity of any financial indebtedness;
3. any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;
4. the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or
5. the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;

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

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

### 4. Consequences of Financial Distress events

4.1 Immediately upon notification by the Supplier of a Financial Distress Event (or if the Relevant Authority becomes aware of a Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and the Relevant Authority shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

4.2 In the event of a late or non-payment of a Key Sub-contractor pursuant to Paragraph 3.1.5, the Relevant Authority shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:

4.2.1 rectify such late or non-payment; or

4.2.2 demonstrate to the Relevant Authority's reasonable satisfaction that there is a valid reason for late or nonpayment.]

4.3 The Supplier shall (and shall procure that any Monitored Supplier, the Guarantor and/or any relevant Key-Subcontractorshall):

4.3.1 at the request of the Relevant Authority meet the Relevant Authority as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) or such other period as the Relevant Authority may permit and notify to the Supplier in writing) to review the effect of the Financial Distress Event on the continued performance and delivery of the Services in accordance with the Contract; and

4.3.2 where the Relevant Authority reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1) that the Financial Distress Event could impact on the continued performance of each Contract and delivery of the Deliverables in accordance with each Call-Off Contract:

1. submit to the Relevant Authority for its Approval, a draft Financial Distress Remediation Plan as soon as reasonably practicable (and in any event, within ten

(10) Working Days of the initial notification (or awareness) of the Financial Distress Event) or such other period as the Relevant Authority may permit and notify to the Supplier in writing; and

1. to the extent that it is legally permitted to do so and subject to Paragraph 4.8, provide such information relating to the Supplier, any Monitored Supplier, Key SubContractors and/or the Guarantor as the Buyer may reasonably require in order to understand the risk to the Deliverables, which may include forecasts in relation to cash flow, orders and profits and details of financial measures being considered to mitigate the impact of the Financial Distress Event.
   1. The Relevant Authority shall not withhold its approval of a draft Financial Distress Remediation Plan unreasonably.If the Relevant Authority does not approve the draft Financial Distress RemediationPlan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress RemediationPlan, which shall be resubmitted to the Relevant Authority within five (5) Working Days of the rejection of the first draft. This process shall be repeated until the Financial Distress RemediationPlan is approved by the Relevant Authority or referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms under Paragraph 4.5.
   2. If the Relevant Authority considers that the draft Financial Distress

RemediationPlan is insufficiently detailed to be properly evaluated, will take too long to complete or will not ensure the continued performance of the Supplier’s obligations in accordance with the Contract, then it may either agree a further time period for the development and agreement of the Financial Distress Remediation Plan or escalate any issues with the draft Financial Distress Remediation Plan using the Dispute Resolution Procedure in Clause 34 of the Core Terms.

* 1. Following Approval of the Financial Distress RemediationPlan by CCS, the Supplier shall:

4.6.1 on a regular basis (which shall not be less than fortnightly)

(a) review and make any updates to the Financial Distress Remediation Plan as the Supplier may deem reasonably necessary and/or as may be reasonably requested by the Relevant Authority, so that the plan remains adequate,

up to date and ensures the continued performance and delivery of the Deliverables in accordance with Contract; and

4.6.2 where updates are made to the Financial Distress

Remediation Plan in accordance with Paragraph 4.6.1, submit an updated Financial Distress RemediationPlan to the Relevant Authority for its approval, and the provisions of Paragraphs 4.4 and 4.5 shall apply to the review and approval process for the updated Financial Distress Remediation Plan; and

4.6.3 comply with the Financial Distress Remediation Plan (including any updated Financial Distress Remediation Plan) and ensure that it achieves the financial and performance requirements set out in the Financial Distress Remediation Plan.

4.7 Where the Supplier reasonably believes that the relevant Financial Distress Event under Paragraph 4.1 (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Relevant Authority and the Parties may agree that the Supplier shall be relieved of its obligations under Paragraph 4.6.

4.8 The Supplier shall use reasonable endeavours to put in place the necessary measures to ensure that the information specified at paragraph 4.3.2(b) is available when required and on request from the Relevant Authority and within reasonable timescales. Such measures may include:

4.8.1 obtaining in advance written authority from Key Subcontractors, the Guarantor and/or Monitored Suppliers authorising the disclosure of the information to the Buyer and/or entering into confidentiality agreements which permit disclosure;

4.8.2 agreeing in advance with the Relevant Authority, Key Subcontractors, the Guarantor and/or Monitored Suppliers a form of confidentiality agreement to be entered by the relevant parties to enable the disclosure of the information to the Relevant Authority;

4.8.3 putting in place any other reasonable arrangements to enable the information to be lawfully disclosed to the Relevant Authority (which may include making price sensitive information available to the Relevant Authority’s nominated personnel through confidential arrangements, subject to their consent); and

4.8.4 disclosing the information to the fullest extent that it is lawfully entitled to do so, including through the use of redaction, anonymisation and any other techniques to permit disclosure of the information without breaching a duty of confidentiality.

### 5. Financial Indicators

#### 5.1 Subject to the calculation methodology set out at Annex 3 of this

**Schedule, the Financial Indicators and the corresponding calculations and**

**thresholds used to determine whether a Financial Distress Event has occurred in respect of those Financial Indicators, shall be as follows:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Financial Indicator** | **Calculation1** | **Financial**  **Target**  **Threshold:** | **Monitoring and**  **Reporting Frequency if different from the**  **default position set out in Paragraph 2.3.2** |
| **1**  **Operating Margin** | ***[Operating***  ***Margin =***  ***Operating Profit***  ***/ Revenue]*** | ***>5%*** | ***As set out in paragraph***  ***2.3.2*** |
| **2**  **Net Debt Ratio** | ***[Net Debt to***  ***EBITDA ratio =***  ***Net Debt /***  ***EBITDA]*** | ***< 3.5 times*** | ***As set out in paragraph***  ***2.3.2*** |
| **3**  **Net Debt + Net**  **Pension Deficit to**  **EBITDA ratio** | ***[Net Debt + Net Pension Deficit to EBITDA Ratio***  ***= (Net Debt + Net Pension***  ***Deficit) /***  ***EBITDA]*** | ***< 5.0 times*** | ***As set out in paragraph***  ***2.3.2*** |
| **4**  **Net Interest Paid**  **Cover** | ***[Net Interest***  ***Paid Cover =***  ***Earnings Before***  ***Interest and Tax***  ***/ Net Interest Paid]*** | ***> 3.0 times*** | ***As set out in paragraph***  ***2.3.2*** |
| **5**  **Acid Ratio** | ***[Acid Ratio =***  ***(Current Assets***  ***– Inventories) / Current***  ***Liabilities]*** | ***> 0.8*** | ***As set out in paragraph***  ***2.3.2*** |
| **6**  **Net Asset value** | ***[Net Asset***  ***Value = Net Assets]*** | ***> £0*** | ***As set out in paragraph***  ***2.3.2*** |
| **7**  **Group Exposure**  **Ratio** | ***[Group***  ***Exposure /***  ***Gross Assets]*** | ***< 50%*** | ***As set out in paragraph***  ***2.3.2*** |

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

#### 5.2Monitored Suppliers

|  |  |
| --- | --- |
| **Monitored Supplier** | **Applicable Financial Indicators**  **(these are the Financial Indicators from the table in section 5.1 which are to apply to the Monitored**  **Suppliers)** |
| **Guarantor** | 1. **- Operating Margin** 2. **-Net Debt Ratio** 3. **- Net Debt + Net Pension Deficit to EBITDA ratio** 4. **- Net Interest Paid Cover** 5. **- Acid Ratio** 6. **- Net Asset value** 7. **- Group Exposure Ratio** |
| **Key sub-contractor** | 1. **- Operating Margin** 2. **-Net Debt Ratio** 3. **- Net Debt + Net Pension Deficit to EBITDA ratio** 4. **- Net Interest Paid Cover** 5. **- Acid Ratio** 6. **- Net Asset value** 7. **- Group Exposure Ratio** |

### 6. Termination Rights

6.1 The Relevant Authority shall be entitled to terminate the Contract if:

6.1.1 the Supplier fails to notify the Relevant Authority of a Financial Distress Event in accordance with Paragraph 2.3.3;

6.1.2 the Parties fail to agree a Financial Distress Remediation Plan (or any updated Financial Distress RemediationPlan) in accordance with Paragraphs 4.3 to 4.5; and/or

6.1.3 the Supplier fails to comply with the terms of the Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraph 4.6.3.

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

6.2 If the Contract is terminated in accordance with Paragraph 5.1, Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply as if the Contract had been terminated under Clause 10.4.1.

### 7. Primacy of Credit Ratings

7.1 Without prejudice to the Supplier’s obligations and the Relevant Authority’s rights and remedies under Paragraph 2, if, following the occurrence of a Financial Distress Event, pursuant to any of Paragraphs 3.1.2 to 3.1.7, the

Rating Agencies review and report subsequently that the credit ratings for the FDE Group entities do not drop below the relevant Credit Rating Thresholds specified for those entities in Annex 2 to this Schedule,, then:

7.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and

7.1.2 the Relevant Authority shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

### 8.Board confirmation

8.1If the Contract has been specified as a Critical Service Contract under

Paragraph 1.1 of Part B of Annex 1 to Call-Off Schedule 8 (Business

Continuity and Disaster Recovery) (if applicable) then, subject to Paragraph

8.4 of this Schedule, the Supplier shall within ninety (90) days after each Accounting Reference Date or within 15 months of the previous Board

Confirmation (whichever is the earlier) provide a Board Confirmation to the Relevant Authority in the form set out at Annex 4 to this Schedule, confirming that to the best of the Board’s knowledge and belief, it is not aware of and has no knowledge:

8.1.1that a Financial Distress Event has occurred since the later of the Effective Date or the previous Board Confirmation or is subsisting; or

8.1.2of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event.

8.2The Supplier shall ensure that in its preparation of the Board Confirmation it exercises due care and diligence and has made reasonable enquiry of all relevant Supplier Staff and other persons as is reasonably necessary to understand and confirm the position.

8.3In respect of the first Board Confirmation to be provided under this Contract, the Supplier shall provide the Board Confirmation within 15 months of the Effective Date if earlier than the timescale for submission set out in Paragraph 8.1 of this Schedule.

8.4Where the Supplier is unable to provide a Board Confirmation in accordance with Paragraphs 8.1 to 8.3 of this Schedule due to the occurrence of a Financial Distress Event or knowledge of subsisting matters which could reasonably be expected to cause a Financial Distress Event, it will be sufficient for the Supplier to submit in place of the Board Confirmation, a statement from the Board of Directors to the Buyer (and where the Supplier is a Strategic Supplier, the Supplier shall send a copy of the statement to the Cabinet Office Markets and Suppliers Team) setting out full details of any Financial Distress Events that have occurred and/or the matters which could reasonably be expected to cause a Financial Distress Event.

### 9. Optional Clauses

9.1 Where a Buyer’s Call-Off Contract is a Bronze Contract, if specified in the Order Form, the terms at Annex 5 shall apply to the Call-Off Contract in place of the foregoing terms of this Joint Schedule 7.

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

Dun & Bradstreet

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

|  |  |
| --- | --- |
| **Entity** | **Credit rating (long term)** |
| Supplier | 30 |
| Guarantor | 30 |
| Key sub-contractor | 30 |

### Annex 3: Calculation methodology for Financial Indicators

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

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

### Specific Methodology

|  |  |
| --- | --- |
| **Financial Indicator** | Specific Methodology |
| **1**  **[Operating Margin]** | [The elements used to calculate the Operating Margin should be shown on the face of the Income Statement in a standard set of financial statements.  Figures for Operating Profit and Revenue should exclude the entity’s share of the results of any joint ventures or Associates.  Where an entity has an operating loss (i.e. where the operating profit is negative), Operating Profit should be taken to be zero.] |

|  |  |
| --- | --- |
| **2**  **[Free Cash Flow to**  **Net Debt Ratio]** | *[“****Free Cash Flow****” = Net Cash Flow from Operating*  *Activities – Capital Expenditure*  *“****Capital Expenditure****” = Purchase of property, plant & equipment + purchase of intangible assets*  *“****Net Debt****” = Bank overdrafts + Loans and borrowings + Finance Leases + Deferred consideration payable – Cash and cash equivalents*  The majority of the elements used to calculate the Free Cash Flow to Net Debt Ratio should be shown on the face of the Statement of Cash Flows and the Balance Sheet in a standard set of financial statements.  *Net Cash Flow from Operating Activities*: This should be stated after deduction of interest and tax paid.  *Capital expenditure*: The elements of capital expenditure may be described slightly differently but will be found under ‘Cash flows from investing activities’ in the Statement of Cash Flows; they should be limited to the purchase of fixed assets (including intangible assets) for the business and exclude acquisitions. The figure should be shown gross without any deduction for any proceeds of sale of fixed assets.  *Net Debt*: The elements of Net Debt may also be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest bearing liabilities (other than retirement benefit obligations) should be treated as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but not non-designated hedges). Borrowings should also include balances owed to other group members.  Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing.  Cash and cash equivalents should include short-term financial investments shown in current assets.  Where Net debt is negative (i.e. an entity has net cash), the relevant Financial Target Threshold should be treated as having been met.]  OR |

|  |  |
| --- | --- |
| **OR**  **[Net Debt to EBITDA**  **Ratio]** | *[“****Net Debt****” = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents*  *“****EBITDA****” = Operating profit + Depreciation charge + Amortisation charge*  The majority of the elements used to calculate the Net Debt to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement and Statement of Cash Flows in a standard set of financial statements but will otherwise be found in the notes to the financial statements.  *Net Debt*: The elements of Net Debt may be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest bearing liabilities (other than retirement benefit obligations) should be included as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but not non-designated hedges). Borrowings should also include balances owed to other group members.  Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing.  Cash and cash equivalents should include short-term financial investments shown in current assets.  Where Net debt is negative (i.e. an entity has net cash), the relevant Financial Target Threshold should be treated as having been met.  *EBITDA*: Operating profit should be shown on the face of the Income Statement and, for the purposes of calculating this Financial Indicator, should include the entity’s share of the results of any joint ventures or Associates. *The depreciation and amortisation charges for the period may be found on the face of the Statement of Cash Flows or in a Note to the Accounts. Where EBITDA is negative, the relevant Financial Target Threshold should be treated as not having been met (unless Net Debt is also negative, in which case the relevant Financial Target Threshold should be treated as having been met).]* |

|  |  |  |
| --- | --- | --- |
| **3**  **[Net Debt +**  **Pension Deficit**  **EBITDA ratio]** | **Net to** | *[“****Net Debt****” = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents*  *“****Net Pension Deficit****” = Retirement Benefit Obligations – Retirement Benefit Assets*  *“****EBITDA****” = Operating profit + Depreciation charge + Amortisation charge*  The majority of the elements used to calculate the Net Debt + Net Pension Deficit to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement and Statement of Cash Flows in a standard set of financial statements but will otherwise be found in the notes to the financial statements.  *Net Debt*: The elements of Net Debt may be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest bearing liabilities (other than retirement benefit obligations) should be included as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but *not* non-designated hedges). Borrowings should also include balances owed to other group members.  Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing.  Cash and cash equivalents should include short-term financial investments shown in current assets.  *Net Pension Deficit*: Retirement Benefit Obligations and Retirement Benefit Assets may be shown on the face of the Balance Sheet or in the notes to the financial statements. They may also be described as pension benefits / obligations, post-employment obligations or other similar terms.  Where ‘Net Debt + Net Pension Deficit’ is negative, the relevant Financial Target Threshold should be treated as having been met.  *EBITDA*: Operating profit should be shown on the face of the Income Statement and, for the purposes of calculating this Financial Indicator, should include the entity’s share of the results of any joint ventures or Associates. |

|  |  |
| --- | --- |
|  | The depreciation and amortisation charges for the period may be found on the face of the Statement of Cash Flows or in a Note to the Accounts.  Where EBITDA is negative, the relevant Financial Target Threshold should be treated as not having been met (unless ‘Net Debt + Net Pension Deficit’ is also negative, in which case the relevant Financial Target Threshold should be regarded as having been met).] |

|  |  |  |  |
| --- | --- | --- | --- |
| **4**  **[Net Interest**  **Cover]** | | **Paid** | *[“****Earnings Before Interest and Tax****” = Operating profit*  *“****Net Interest Paid****” = Interest paid – Interest received*  Operating profit should be shown on the face of the Income Statement in a standard set of financial statements and, for the purposes of calculating this Financial Indicator, should include the entity’s share of the results of any joint ventures or Associates.  Interest received and interest paid should be shown on the face of the Cash Flow statement.  Where Net interest paid is negative (i.e. the entity has net interest received), the relevant Financial Target Threshold should be treated as having been met.] |
| **5**  **[Acid Ratio]** | |  | [All elements that are used to calculate the Acid Ratio are available on the face of the Balance Sheet in a standard set of financial statements.] |
| **6**  **[Net Asset value]** | | | [Net Assets are shown (but sometimes not labelled) on the face of the Balance Sheet of a standard set of financial statements. Net Assets are sometimes called net worth or ‘Shareholders’ Funds’. They represent the net assets available to the shareholders. Where an entity has a majority interest in another entity in which there are also minority or non-controlling interests (i.e. where it has a subsidiary partially owned by outside investors), Net Assets should be taken inclusive of minority or noncontrolling interests (as if the entity owned 100% of such entity).] |
| **7**  **[Group**  **Ratio]** | **Exposure** | | *[“****Group Exposure****” = Balances owed by Group*  *Undertakings + Contingent liabilities assumed in support of Group Undertakings*  *“****Gross Assets****” = Fixed Assets + Current Assets*  *Group Exposure*: Balances owed by (ie receivable from) Group Undertakings are shown within Fixed assets or Current assets either on the face of the Balance Sheet or in the relevant notes to the financial statements. In many cases there may be no such balances, in particular where an entity is not a member of a group or is itself the ultimate holding company of the group.  Contingent liabilities assumed in support of Group Undertakings are shown in the Contingent Liabilities note in a standard set of financial statements. They include guarantees and security given in support of the borrowings of other group companies, often as part of group borrowing arrangements. Where the contingent liabilities are capped, the capped figure should be taken as their value. Where no cap or maximum is specified, the relevant Financial Target Threshold should automatically be regarded as not having been met.  In many cases an entity may not have assumed any contingent liabilities in support of Group Undertakings, in particular where an entity is not a member of a group or is itself the ultimate holding company of the group.  *Gross Assets*: Both Fixed assets and Current assets are shown on the face of the Balance Sheet] |

**ANNEX 4: BOARD CONFIRMATION**

**Supplier Name:**

**Contract Reference Number:**

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

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

1. that a Financial Distress Event has occurred since the later

of the previous Board Confirmation and the Effective Date or is subsisting; or

1. of any matters which have occurred or are subsisting that

could reasonably be expected to cause a Financial Distress Event

On behalf of the Board of Directors:

Chair ………………………………… Signed ………………………………… Date …………………………………

Director ………………………………… Signed ………………………………… Date …………………………………

# ANNEX 5: OPTIONAL CLAUSES FOR BRONZE CONTRACTS

## 1. Definitions

1.1In this Annex 5, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

|  |  |
| --- | --- |
| **"Credit**  **Rating**  **Threshold"** | the minimum credit rating level for  the Monitored Company as set out  in Appendix 2; |
| **"Financial**  **Distress**  **Event"** | the occurrence or one or more of the following events:   1. the credit rating of the Monitored   Company dropping below the applicable  Credit Rating Threshold;   1. the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects; 2. there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party; 3. Monitored Company committing a material breach of covenant to its lenders; 4. a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or |

f) any of the following:

1. commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract;
2. non-payment by the Monitored Company of any financial indebtedness;
3. any financial indebtedness of the

Monitored Company becoming due as a result of an event of default; or

1. the cancellation or suspension of any financial indebtedness in respect of the

Monitored Company in each case which the Relevant Authority reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any

Contract and delivery of the

Deliverables in accordance with any

Call-Off Contract;

|  |  |
| --- | --- |
| **"Financial**  **Distress**  **Service**  **Continuity**  **Plan"** | a plan setting out how the Supplier  will ensure the continued performance and delivery of the Deliverables in accordance with [each Call-Off] Contract in the event that a Financial Distress Event occurs; |
| **“Monitored**  **Company”** | Supplier [the Guarantor] or any Key Subcontractor] |
| **"Rating**  **Agencies"** | the rating agencies listed in Appendix 1. |

## 2. When this Schedule applies

2.1The Parties shall comply with the provisions of this Annex 5 in relation to the assessment of the financial standing of the Monitored Companies and the consequences of a change to that financial standing.

2.2 The terms of this Annex 5 shall survive:

2.2.1under the Framework Contract until the later of (a) the termination or expiry of the Framework Contract or (b) the latest date of termination or expiry of any call-off contract entered into under the Framework Contract (which might be after the date of termination or expiry of the Framework Contract); and

2.2.2under the Call-Off Contract until the termination or expiry of the Call-Off Contract.

## 3. What happens when your credit rating changes

3.1The Supplier warrants and represents to the Relevant Authority that as at the Start Date the long term credit ratings issued for the Monitored Companies by each of the Rating Agencies are as set out in Appendix 2.

3.2The Supplier shall promptly (and in any event within five (5) Working Days) notify the Relevant Authority in writing if there is any downgrade in the credit rating issued by any Rating Agency for a Monitored Company.

3.3If there is any downgrade credit rating issued by any Rating Agency for the Monitored Company the Supplier shall ensure that the Monitored Company’s auditors thereafter provide the Relevant Authority within 10

Working Days of the end of each Contract Year and within 10 Working Days of written request by the Relevant Authority (such requests not to exceed 4 in any Contract Year) with written calculations of the quick ratio for the Monitored Company as at the end of each Contract Year or such other date as may be requested by the Relevant Authority. For these purposes the "quick ratio" on any date means:



where:

1. is the value at the relevant date of all cash in hand and at the bank of the Monitored Company];
2. is the value of all marketable securities held by the Supplier the Monitored Company determined using closing prices on the Working Day preceding the relevant date;
3. is the value at the relevant date of all account receivables of the Monitored]; and
4. is the value at the relevant date of the current liabilities of the Monitored Company].

3.4The Supplier shall:

* + 1. regularly monitor the credit ratings of each Monitored Company with the Rating Agencies; and
    2. promptly notify (or shall procure that its auditors promptly notify) the Relevant Authority in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, ensure

that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

3.5For the purposes of determining whether a Financial Distress Event has occurred the credit rating of the Monitored Company shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated the Monitored Company at or below the applicable Credit Rating Threshold.

## 4. What happens if there is a financial distress event

4.1In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if the Relevant Authority becomes aware of the Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and the Relevant Authority shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6 of this Annex 5.

4.2[In the event that a Financial Distress Event arises due to a Key Subcontractor notifying the Relevant Authority that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute then, the Relevant Authority shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:

4.2.1rectify such late or non-payment; or

4.2.2demonstrate to the Relevant Authority's reasonable satisfaction that there is a valid reason for late or nonpayment.]

4.3The Supplier shall and shall procure that the other Monitored Companies shall:

4.3.1at the request of the Relevant Authority meet the Relevant Authority as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) to review the effect of the Financial

Distress Event on the continued performance of each Contract and delivery of the Deliverables in accordance each Call-Off Contract; and

4.3.2where the Relevant Authority reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1) that the Financial Distress Event could impact on the continued performance of each Contract and delivery of the

Deliverables in accordance with each Call-Off Contract:

1. submit to the Relevant Authority for its Approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within ten (10) Working Days of the initial notification (or awareness) of the Financial Distress Event); and
2. provide such financial information relating to the Monitored Company as the Relevant Authority may reasonably require.
   1. If the Relevant Authority does not (acting reasonably) approve the draft Financial Distress Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to the Relevant Authority within five (5) Working Days of the rejection of the first or subsequent (as the case may be) drafts.

This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by the Relevant Authority or referred to the Dispute Resolution Procedure.

* 1. If the Relevant Authority considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not remedy the relevant Financial Distress Event, then it may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the Dispute Resolution Procedure.
  2. Following Approval of the Financial Distress Service Continuity Plan by the Relevant Authority, the Supplier shall:
     1. on a regular basis (which shall not be less than Monthly), review the Financial Distress Service Continuity Plan and assess whether it remains adequate and up to date to ensure the continued performance each Contract and delivery of the Deliverables in accordance with each Call-Off Contract;
     2. where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1, submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 4.5 and 4.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and
     3. comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).
  3. Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Relevant Authority and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.
  4. CCS shall be able to share any information it receives from the Buyer in accordance with this Paragraph with any Buyer who has entered into a Call-Off Contract with the Supplier.

## 5. When CCS or the Buyer can terminate for financial distress

5.1CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:

5.1.1the Supplier fails to notify the Relevant Authority of a Financial Distress Event in accordance with Paragraph

3.4;

5.1.2The Relevant Authority and the Supplier fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 4.3 to 4.5; and/or

5.1.3the Supplier fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraph 4.6.3.

5.2If the Contract is terminated in accordance with Paragraph 5.1, Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply as if the Contract had been terminated under Clause 10.4.1.

**6.** **What happens If your credit rating is still good** 6.1 Without prejudice to the Supplier’s obligations and CCS’ and the Buyer’s rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:

6.1.1the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and

6.1.2The Relevant Authority shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

## APPENDIX 1: RATING AGENCIES

[Rating Agency 1]

[Rating Agency 2]

## APPENDIX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

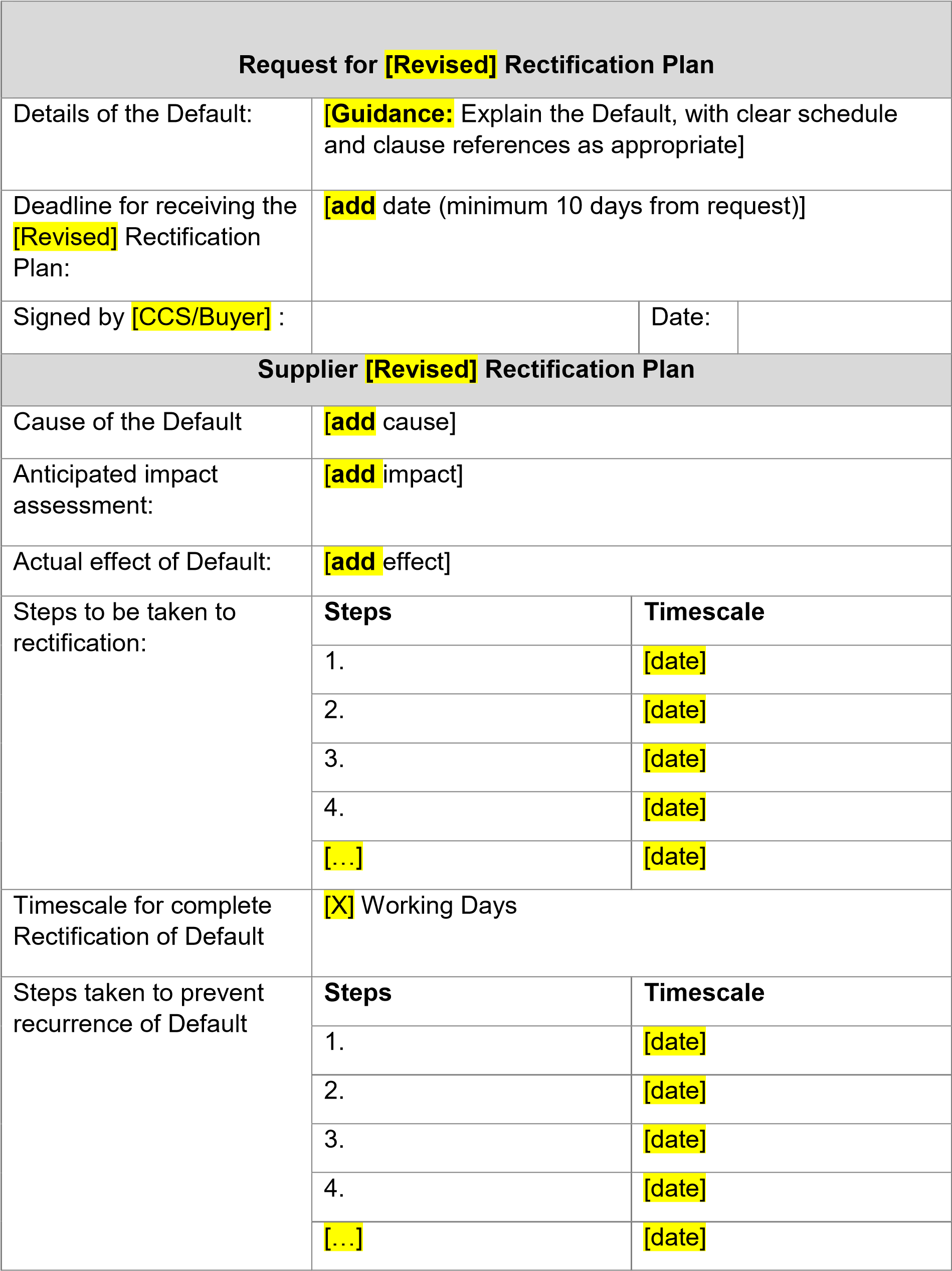
### Part 1: Current Rating

|  |  |  |
| --- | --- | --- |
| **Entity** | **Credit rating (long term)** |  |
| Supplier | [D&B Threshold] |  |
| [Guarantor] |  |  |
| [Key Subcontractor] |  |  |

**Joint Schedule 10 (Rectification Plan)**

Crown Copyright2018

## Joint Schedule 10 (Rectification Plan)



Framework Ref: RM6116

Project Version: v1.0 2

Model Version: v3.0

**Joint Schedule 10 (Rectification Plan)**

Crown Copyright2018

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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: | |  | |
|  |

Framework Ref: RM6116

Project Version: v1.0 2

Model Version: v3.0

## Joint Schedule 11 (Processing Data)

### Definitions

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

**“Processor** all directors, officers, employees, agents, consultants and

**Personnel”** suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

### Status of the Controller

2. 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 2018. A Party may act as:

(a) “Controller” in respect of the other Party who is “Processor”; (b) “Processor” in respect of the other Party who is “Controller”;

1. “Joint Controller” with the other Party;
2. “Independent Controller” of the Personal Data where the other Party is also

“Controller”,

in respect of certain Personal Data under a Contract and shall specify in Annex 1 of this Joint Schedule 11 *(Processing Personal Data)* which scenario they think shall apply in each situation.

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

1. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 of this Joint Schedule 11 *(Processing Personal Data*) by the Controller.
2. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
3. 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:
4. a systematic description of the envisaged Processing and the purpose of the Processing;
5. an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
6. an assessment of the risks to the rights and freedoms of Data Subjects; and
7. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

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

1. Process that Personal Data only in accordance with Annex 1 of this Joint Schedule 11 *(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;
2. 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:
   1. nature of the data to be protected;
   2. harm that might result from a Personal Data Breach;
   3. state of technological development; and
   4. cost of implementing any measures; (c) ensure that :
   5. the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1of this Joint Schedule 11 *(Processing Personal Data*));
   6. 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:
      1. 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*) of the Core Terms;
      2. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
      3. 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
      4. have undergone adequate training in the use, care, protection and handling of Personal Data;
3. not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
   1. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
   2. the Data Subject has enforceable rights and effective legal remedies;
   3. 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
   4. 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
4. 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.

7. Subject to paragraph 8 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:

1. receives a Data Subject Access Request (or purported Data Subject Access Request);
2. receives a request to rectify, block or erase any Personal Data;
3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
5. 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
6. becomes aware of a Personal Data Breach.
7. The Processor’s obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
8. 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 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
9. the Controller with full details and copies of the complaint, communication or request;
10. 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;
11. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
12. assistance as requested by the Controller following any Personal Data Breach; and/or
13. 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.

10. 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:

1. the Controller determines that the Processing is not occasional;
2. the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
3. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
4. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller’s designated auditor.
5. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
6. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
7. notify the Controller in writing of the intended Subprocessor and Processing;
8. obtain the written consent of the Controller;
9. 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
10. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
11. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
12. The Relevant Authority may, at any time on not less than thirty (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).
13. The Parties agree to take account of any guidance issued by the Information

Commissioner’s Office. 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’s Office.

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

17. 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 UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

### Independent Controllers of Personal Data

1. 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.
2. 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.
3. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 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.
4. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
5. The Parties shall only provide Personal Data to each other:
6. to the extent necessary to perform their respective obligations under the Contract;
7. 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 UK GDPR); and
8. where it has recorded it in Annex 1 of this Joint Schedule 11 *(Processing Personal Data).*
9. 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 UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
10. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
11. 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”)**:
12. 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
13. 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:
    1. 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
    2. 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.

26. 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:

1. do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
2. implement any measures necessary to restore the security of any compromised Personal Data;
3. 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

1. 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.
2. 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 of this Joint Schedule 11 *(Processing Personal Data).*
3. 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 of this Joint Schedule 11 *(Processing Personal Data)*.
4. Notwithstanding the general application of paragraphs 2 to 16 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 paragraphs 18 to 28 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.

1.1 The contact details of the Relevant Authority’s Data Protection Officer are:

1.2 The contact details of the Supplier’s Data Protection Officer are: **[Insert** Contact details]

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

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

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of  Controller for each  Category of  Personal Data | **The Relevant Authority is Controller and the Supplier is Processor**  The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 of this Joint Schedule 11 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:  *For the setting up of a Framework. The personal data scope would be business contact details of suppliers and CCS personnel.*  HSE is the controller  Supplier is the processor |
| Duration of the Processing | *For CCS under the Framework Agreement: For up to* ***4*** *years corresponding with a* ***2*** *year framework term and* ***2*** *optional* ***12*** *month extensions.*  *Then for 7 years post framework expiry as per regulatory retention requirements for commercial/financial data.*  *For Buyers:* [The contract will be for 4 years] |
| Nature and purposes of the  Processing | *In respect of the Supplier Personal Data, CCS (and any other Relevant Authority) may: collect, collate, share, evaluate, use, store, replicate, and otherwise Process the Personal Data (subject to the terms of the Contract) to enable it to administer the Contract and fulfil tasks in the public interest and as required by law.* |

|  |  |
| --- | --- |
|  | *This may include:*   * *inviting the Supplier Staff to contract management workshops and events;* * *complying with requirements under the Contract to contact named individuals;* * *establishing the Supplier’s compliance with the procurement process and the Contract; and* * *including Personal Data within reports.*   *In respect of the Relevant Authority’s Personal Data over which the Supplier shall act as a Controller, the Supplier may: collect, collate, share, evaluate, use, store, replicate, and otherwise Process the Personal Data (subject to the terms of the Contract) to enable it to administer and fulfil its obligations under the Contract.*  *This may include:*   * *complying with requirements under the Contract to contact named individuals; and* * *including Personal Data within reports.*     The nature of processing is as follows, this is not exhaustive and may be added to:    **Contact centre:**  Recording and storage of telephone calls for the purpose of monitoring and training of agents and for managers to intercept calls in case of abuse.    Capturing callers names, details of the call and phone numbers for the purpose of calling them back to assist with their query.  Caller can leave a message or request a call back.  Exporting data for management reports.  **Enterprise Telephony** |

|  |  |
| --- | --- |
|  | Billing information – phone number and employee name, call duration and number of calls    Incident and problem management for enterprise telephony or contact centre i.e. troubleshooting between the supplier and HSE user. This may involve a user sharing a screen via a remote desktop application. |
| Type of Personal Data | *Individuals’ names, job titles, email addresses, organisational name, work phone numbers. To the extent relevant and supplied during the procurement process, details of any relevant convictions.*    This personal data list is not exhaustive and may be added to:    **HSE Manager and Agent**   * Name * Work email * Work mobile   **Advice Form** (Contact) CAT Reference   * Date received  Enquirer name * Phone number * Email address * Contact preference  Person type  Person type - other * Postcode * Enquiry Country * Enquiry County * [Control]   Enquir  y Local Authority      [  Control  ]           * Organisation type  Organisation type - other * Raised with HSE before * Previous reference * Advice needed: Up to 3000 characters allowed * COVID related  Action requested * Triaged by |

|  |  |
| --- | --- |
|  | * Topics * Classification * Enquiry theme * Available for feedback * Enquiry taken by * Agent full name * Followed up by * Action / Notes / Response: - Up to 10,000 characters allowed * Internal referral / assistance * Date of referral * Date of return * Status * New * Date of closure * Outcome     **Concerns Form** (Contact)     * Date raised * CAT Reference * Notifier name * Notifier email * Notifier phone * Contact preference * Notifier address * Notifier postcode  Country     County      [  Control  ]      Local  Authority      [  Control  ]      Role               * Role - other * Risk activity * Risk of Sickness, injury or death * Action requested * Concern details: - Up to 3000 characters allowed * Likely to be harmed * Employees * Length of work * Length of risk time * Expected future risk time * Raised concern * Aggressive people * Aggressive animals * Violence and Aggression * Photos / Docs * Sharepoint Evidence * Person in charge known |

|  |  |
| --- | --- |
|  | * Person in charge * Company name known * Company name * Activity address * Location description: - Up to 1000 characters allowed * Alternate contact  Type of work at site  Type of work at site: * Can we say an issue has been raised * Can we give your name * Raised with HSE before * Previous reference * Team Allocation * Allocated to * Is it a concern for HSE or Other: * Triage filter category: * Covid related * Covid Theme * Covid Theme (Other) * Decision / Action / Notes: - Up to 10,000 characters allowed  Actioned by CAT / Field / Other: * Current status * Closed outcome: * CSO Referral / Action completed by: * Notifier feedback complete: * Date closed * Letter number * Coin case number * FOD Group * Reason referred to field  PI returned to CAT     **Building Safety Regulator contact**    **Contact Details:**   * First Name * Last Name * Job Title * Account Name * E-mail * Mobile Phone * Business Phone * Address   Note – not all fields may be completed    Building Details – if the contact is regarding a specific high rise building |

|  |  |
| --- | --- |
|  | Complaint About – if the contact is regarding a specific person or organisation  Case Summary - Description  Role – e.g.:   * Resident * Member of the public * Third party * Building professional * Other     **Support calls**  Desktop screen sharing for troubleshooting in relation to incident management.  HSE staff name, email address and telephone number. |
| Categories of Data Subject | *Relevant Authority Staff and Supplier Staff.*  Members of the public  HSE duty holders  Employees from other government departments  HSE employees |
| Plan for return and destruction of the data once the Processing is complete  UNLESS  requirement under  Union or Member  State law to | *For the duration of the Contract and 7 years after.*    Prior to exit of contract HSE expects that the data is returned (exported) or destroyed at no extra cost to HSE.  HSE will instruct at the time. |
| preserve that type of data |  |

### 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 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 18-28 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]:

1. is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
2. 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;
3. is solely responsible for the Parties’ compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
4. is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and
5. 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.

#### 2. Undertakings of both Parties

2.1 The Supplier and the Relevant Authority each undertake that they shall:

1. report to the other Party every [number of months] months on:
   1. the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
   2. the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
   3. 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;
   4. any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
   5. 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;

1. notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
2. 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;
3. not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables 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;
4. request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
5. 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;
6. 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:
   1. are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;
   2. 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 that Party would not be permitted to do so; and
   3. have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
7. ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
8. nature of the data to be protected;
   1. harm that might result from a Personal Data Breach;
   2. state of technological development; and
   3. cost of implementing any measures;
9. 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
10. 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 other Party and its advisors with:

1. 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; and
2. all reasonable assistance, including:
   * 1. 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;
     2. co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
     3. co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
     4. 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:

1. the nature of the Personal Data Breach;
2. the nature of Personal Data affected;
3. the categories and number of Data Subjects concerned;
4. the name and contact details of the Supplier’s Data Protection Officer or other relevant contact from whom more information may be obtained;
5. measures taken or proposed to be taken to address the Personal Data Breach; and
6. describe the likely consequences of the Personal Data Breach.

#### 4. Audit

4.1 The Supplier shall permit:

1. 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
2. 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 UK 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 Deliverables.

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:

1. 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

1. 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 UK 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:

1. 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;
2. 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
3. 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).
   1. 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.
   2. In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the “Claim Losses”):
4. if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;
5. if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
6. 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

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

1. 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
2. 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.

## Joint Schedule 12 (Supply Chain Visibility)

### 1. Definitions

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

**"Contracts Finder"** the Government’s publishing portal for public sector procurement opportunities;

**"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 sized enterprises;

**“Supply Chain Information** the document at Annex 1 of this Schedule

### Report Template” 12; and

**"VCSE"** a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives.

#### 2. Visibility of Sub-Contract Opportunities in the Supply Chain

2.1 The Supplier shall:

2.1.1 subject to Paragraph 2.3, advertise on Contracts Finder all Sub-Contract opportunities arising from or in connection with the provision of the Deliverables above a minimum threshold of £25,000 that arise during the Contract Period;

2.1.2 within 90 days of awarding a Sub-Contract to a Subcontractor, update the notice on Contract Finder with details of the successful Subcontractor;

2.1.3 monitor the number, type an

2.1.4 d value of the Sub-Contract opportunities placed on Contracts Finder advertised and awarded in its supply chain during the Contract Period; 2.1.5 provide reports on the information at Paragraph 2.1.3 to the Relevant

Authority in the format and frequency as reasonably specified by the Relevant Authority; and

2.1.6 promote Contracts Finder to its suppliers and encourage those organisations to register on Contracts Finder.

2.2 Each advert referred to at Paragraph 2.1.1 of this Schedule 12 shall provide a full and detailed description of the Sub-Contract opportunity with each of the mandatory fields being completed on Contracts Finder by the Supplier.

2.3 The obligation on the Supplier set out at Paragraph 2.1 shall only apply in respect of Sub-Contract opportunities arising after the Effective Date.

2.4 Notwithstanding Paragraph 2.1, the Authority may by giving its prior Approval, agree that a Sub-Contract opportunity is not required to be advertised by the Supplier on Contracts Finder.

#### 3. Visibility of Supply Chain Spend

3.1 In addition to any other management information requirements set out in the Contract, the Supplier agrees that where the Relevant Authority is a central government body, and the contract value is worth more than £5 million per year, the Supplier agrees and acknowledges that it shall, at no charge, provide timely, full, accurate and complete SME management information reports (the “SME Management Information Reports”) to the Relevant Authority which incorporates the data described in the Supply Chain Information Report Template which is:

1. the total contract revenue received directly on the Contract;
2. the total value of sub-contracted revenues under the Contract

(including revenues for non-SMEs/non-VCSEs); and

1. the total value of sub-contracted revenues to SMEs and VCSEs.

* 1. The SME Management Information Reports shall be provided by the Supplier in the correct format as required by the Supply Chain Information Report Template and any guidance issued by the Relevant Authority from time to time. The Supplier agrees that it shall use the Supply Chain Information Report Template to provide the information detailed at Paragraph 3.1(a) –(c) and acknowledges that the template may be changed from time to time (including the data required and/or format) by the Relevant Authority issuing a replacement version. The Relevant Authority agrees to give at least thirty (30) days’ notice in writing of any such change and shall specify the date from which it must be used.

* 1. The Supplier further agrees and acknowledges that it may not make any amendment to the Supply Chain Information Report Template without the prior Approval of the Authority.

**Annex 1**

### Supply Chain Information Report template



## Call-Off Schedule 3 (Continuous Improvement)

### 1. Buyer’s Rights

1.1 This Schedule shall apply only when so specified by a Buyer that has undertaken a Further Competition.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.

### 2. Supplier’s Obligations

2.1 The Supplier shall have an ongoing obligation throughout the Contract Period, to identify new or potential improvements to the provision of the Deliverables in accordance with this Call Off Schedule 3 with a view to reducing the Buyer’s costs (including the Call-Off Contract Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer. As part of this obligation the Supplier shall identify and report to the Buyer once every twelve (12) months regarding:

2.1.1 the emergence of new and evolving relevant technologies which could improve the ICT Environment and/or the provision of the Deliverables, and those technological advances potentially available to the Supplier and the Buyer which the Parties may wish to adopt;

2.1.2 new or potential improvements to the Deliverables or the provision of the Deliverables including in respect of the quality, responsiveness, procedures, benchmarking methods, ways of performing the Services and customer support services in relation to the Deliverables;

2.1.3 changes in business processes and working practices that would enable the Deliverables to be provided at lower cost and/or with greater benefits to the Buyer;

2.1.4 changes to the ICT Environment, business processes and working practices that would enable reductions in the total energy consumed in the provision of the Deliverables;

2.1.5 improvements which the Supplier uses or is planning to use with its other customers;

2.1.6 proposals as to how any investment required for continuous improvement could be shared with other customers of the Supplier;

2.1.7 a zero usage report to identify opportunities for cost avoidance;

2.1.8 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;

2.2 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.

2.3 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.

2.4 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.

2.5 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.

2.6 If the Buyer wishes to incorporate any improvement identified by the Supplier into this Contract,including any impact on the Charges declared by the Supplier as part of that improvement, 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.

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

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

2.7.2 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.

2.8 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.

2.9 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.

2.10 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.

2.11 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.

2.12 Notwithstanding anything to the contrary in this Call-Off Contract, the Parties may not change or improve the Deliverables in any way which adversely affects or may adversely affect any relevant PSN Standards or HSCN obligations and processes.

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

**[**[**Guidance:** This Schedule should be used where the Supplier provides a proposal which the Buyer wants the Supplier to be bound by because it may include elements that are either (i) additional to the Call Off Order requirements; or (ii) indicate a specific methods of achieving the Call Off Order requirements. i.e. where the Further Competition Procedure is used.]

**[As specified in our tender response]**

Our employees’ wellbeing is at the core of our ethos. Being a good employer means people will want to work for us, want to develop their career with us and feel motivated to deliver the best service to our clients. We look after our people because it is the right thing to do.

We already provide a comprehensive range of support options, that cover both physical and mental wellbeing. Our approach is both responsive to issues people may be experiencing and proactive in encouraging a healthy lifestyle, work-life balance, and management of stress. As well as providing formal support options, we aim to continually review and refresh the ways in which we can support our workforce and we encourage everyone to be engaged and empowered to take care of their own well-being and look out for their colleagues.

As a business our values of **Grow, Innovate, Collaborate, Trust and Respect** act as the guiding principles for everything we do, our service delivery, products, and our commitment to Social Value.

The Unify Social Value Strategy focuses on issues which support our commitment to wellbeing. The themes are:

* Closing the digital skills gap for all - delivering inclusive and accessible solutions to bridge the digital skills gap.
* Investing in people, inclusion, and wellbeing – Empowering our people to achieve our vision for communities and planet.
* Supporting Communities – Supporting activities which strengthen communities.
* Doing Business Responsibly - having a strong governance, ethics, and compliance approach in everything we do. Responsible procurement is one of our key objectives.

As a business, we have the right skills and expertise to support on the delivery of our Social Value objectives, but partner with local expert partners and organisations to deliver measurable Social Value.

**Our Specific Commitments with regards to Wellbeing**

During the delivery of the Contact Center and Enterprise Telephony project, we are committed to:

|  |  |
| --- | --- |
| 1 | Ensuring all our staff have access to a comprehensive package of wellbeing support via the Unify Wellbeing Village |
| 2 | Supporting and funding our project staff or supply chain to become Mental Health First Aiders |
| 3 | Rolling out one online seminar per year to our project staff and supply chain on subjects such as stress, lifestyle, exercise, and depression. |
| 4 | Working with our recruitment partners and external recruitment agencies to ensure we recruit from a diverse talent pool. |
| 5 | Implementing flexible working hours to allow our staff to have a healthy worklife balance. |
| 6 | Encouraging our staff to volunteer via the Annual Unify Serve Day and Citizen Day so they can spend time in communities. |
| 7 | Arranging mental health initiatives during Mental Health Week to promote the signs, symptoms, and resources available to our staff. |
| 8 | Being a signatory to the Mental Health at Work Charter and developing a robust plan and empowering our staff. |
| 9 | Monitoring wellbeing through our annual employee engagement survey. |

**Method Statement**

Optimising people’s wellbeing is integral to our purpose. We recognise the pivotal role businesses have in making sure health and wellbeing is embedded in our everyday management practices which in turn will improve productivity across the UK economy. The latest estimates from the Labour Force Survey (LFS) show that the rate of cases of workrelated stress, depression or anxiety continue to increase in the UK, and during the pandemic mental health worsened by nearly 10%. As part of our annual Corporate Social Responsibility reporting, we capture elements associated to Wellbeing to our Executive team.

Unify invests in a range of initiatives that proactively support wellbeing. These range from global programmes across our organisation filtering down to local/regional programmes and even further to grassroots initiatives such as 20 minutes, 3 times a week for desk stretching or Office Yoga, to some conference calls being run as a walk and talk while employees are encouraged to participate whilst outside in a green space during the call.

**Annual Wellness Calendar** – this is our schedule of events across the year to address wellness topics



In 2023 there was 9.58 million people of working age (16-64) registered as disabled with 5.15 million in employment. Over the past 2 years the unemployment rate of those registered disabled remains unchanged therefore companies like us recognise the role we can play in empowering and encouraging those with disabilities back into work. Our approach will build on the themes and programmes of our social value strategy. Commitments include:

**All our staff have access to a comprehensive package of wellbeing support via the Unify Wellbeing Village.**

Our strategy aims at being an equal opportunities employer where diversity, equity and inclusion are embedded in everything we do. Our inclusive recruitment practices ensure we are fair but importantly attract and source from a more diverse field. Internally we provide support and training to recruiting managers and the wider business on EDI which includes support for those with disabilities and long-term health conditions. We also provide peer to peer support where appropriate. It will be the responsibility of the SV lead appointed on the project to cascade both our requirements but also promote awareness and support options to our supply chain.

All supply chain members undertake the Unify induction before they start working with us. Through this induction process we support them in sharing any conditions or accessibility requirements they may have. Should we not have the skills internally we will work with local partners to help deliver support or training where required.

**Supporting and funding our project staff or supply chain to become Mental Health First Aiders**

Mental health has a significant impact on the day to day lives of people and manifests itself in a wide range of ways impacting individuals emotionally and mentally. At Unify we recognise the role we must play in ensuring everyone feels psychologically safe and valued. We will support and fund our project staff and supply chain to become mental health first aiders, giving them the tools to support colleagues where required.

**Rolling out one online seminar/article per year/month to our project staff and supply chain on subjects such as stress, lifestyle, exercise, and depression**

Through the Unify Wellness village we have a significant range of resources to support our people on issues ranging from stress, wellbeing, lifestyle, exercise etc. We will commit to running one online seminar alongside our wider suite of resources on specific topics. For example, in June 2024 we published an article on Healthy Skin and Sun Damage Prevention, in May 2024 we published an article on Dental Health. Following these wellness topic articles/webinars we run a brief survey with employees to allow our People and Culture team to develop helpful resources for employees.

**Working with our recruitment partners and external recruitment agencies to ensure we recruit from a diverse talent pool**.

Most of the delivery of our services and products are undertaken remotely therefore limiting the requirement for new roles to be created. However, we also recognise the importance of supporting those with disabilities into the wider Unify family.

Our inclusive recruitment practices mean that no one will be discriminated based on their disabilities or long-term health problem. We will highlight this commitment in all applicable vacancies to demonstrate our commitment to disability inclusion. We will also advertise all job opportunities on websites such as Evenbreak (an accessible job site for people with disabilities).

Between 15-20% of people in the UK are consider neurodivergent which provides great opportunities for employers to harness different thinking styles. The purpose led company called WithYouWithMe advertise re training opportunities to people with neurodiverse conditions. Also, the social enterprise Auticom provide autistic talent and resources to IT businesses across the UK. We will work with all the organisations to attract diverse talent to our business and contracts.

For interviews we will provide reasonable adjustments such as accessible interviews, prep calls with candidates, video calls or interviews avoiding busy travel times. Our roles include a range of working hours and days making them suitable for people with fluctuating health conditions. Unify has fully remote working and this provides an ideal situation for people with disability or health conditions.

Through our EDI strategy we encourage our people to declare their disability status or requirements for their role. This ensures we better understand the conditions of our people and provide the most appropriate support or resources.

**Implementing flexible working hours to allow our staff to have a healthy work-life balance.**

Unify is a flexible employer which benefits both our employees and the organisation. With the work we deliver, we provide the resources and tools for a considerable proportion of our staff to work remotely. The health and wellbeing of our staff is vitally important to us which in turn allows us to reap benefits in terms of lower staff turnover and recruiting the best talent. Post Covid 2020 we are now actively encouraging staff to work from offices on a one day a week basis so they can benefit from the relationships and social interaction with co-workers to avoid feelings of isolation and loneliness.

**Encouraging our staff to volunteer via the Annual Unify Serve Day and Citizen Day so they can spend time in communities.**

Unify recognise the power of volunteering to our colleagues from improved team skills, loyalty, productivity, and networking. Our Serve and Citizen Days provide opportunities across two full days for colleagues to volunteering and participate in local activities. Through our partnership with Goodera we can source local volunteering opportunities very easily. Supporting the communities where we live, and work is critical to helping them thrive. All Unify employees are encouraged to volunteer some time in their local communities. In 2023 we delivered 3000 service hours to 60 organisations. Our goal for 2024 is to achieve at least 3,500 service hours with 60 organizations. Employees log their hours and activity with the global team who track progress against our target.

**Being a signatory to the Mental Health at Work Charter and developing a robust plan and empowering our staff.**

Unify has committed to support the Mental Health at Work charter which provides a roadmap to achieving better mental health outcomes for those in work. The charter is a set of actions that any organisation can follow to improve and support the mental health of their people. We will embed the Six Standards of Mental Health at Work within our business decisions and contracts. The Six Standards include:

* **Prioritise mental health**: we will create prioritise mental health, providing a comprehensive Wellbeing Programme to all staff.
* **Promote positive mental health**: our senior leadership team and three allocated Mental Health First Aiders will be positive role models, promoting activities such as World Mental Health Week
* **Drive an open culture**: we will create an open culture where conversations about mental health are encouraged and included in Townhall discussions, helping to drive positive mental health outcomes.
* **Increase organisational capability**: we will partner with third-party specialists in wellbeing and mental health to educate and increase our workforce through a programme of annual webinars
* **Provide tools and support**: we will provide annual training, created by qualified psychologists on subjects such as anxiety and depression, and access to resources/tooling, to support our line managers, and will regularly signpost mental health tools available on our Wellbeing Hub
* **Increase transparency**: to ensure transparency and accountability, we will measure wellbeing in surveys and adapt actions to remain current e.g., cost of living has replaced Covid as a major employee concern.

**Monitoring wellbeing through our annual employee engagement survey**

Unify regularly collects feedback and develops improvement plans to enhance our employee experience. Our annual employee engagement survey allows us to gather anonymised feedback from our employees. We use these results to create more targeted annual engagement plans, embedding health and wellbeing at the heart of delivery. This year our survey was open for completion from March 4-12th 2024. The results of the survey are collated and presented back to our Global Senior Leadership Team for review and an action plan is created. The results are then cascaded to each individual function where committees are formed to craft the action plans to respond to the issues raised. These plans cover 3/6/12/18 months of activity depending on the complexity of the requirements. Results of the Survey and the progress against the action plan created are shared during the year with all staff at our quarterly Town Hall meetings.

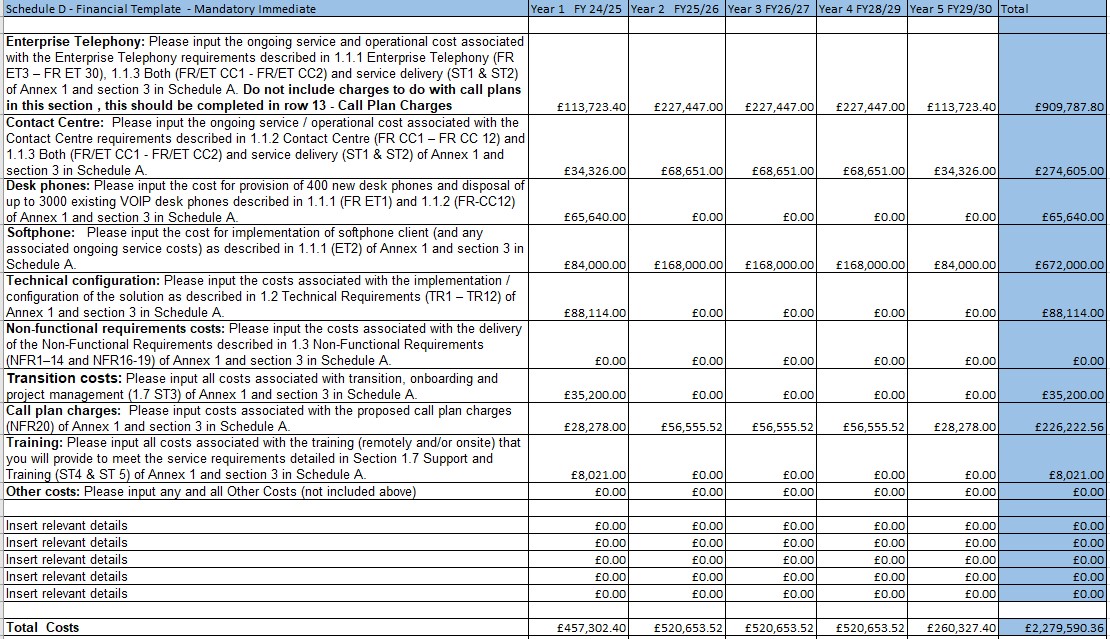
In addition to the annual survey there are several shorter more targeted Pulse Surveys carried out during the year to enable the business to track the effectiveness of the KPIS set to implement changes and improvements to our wellbeing provision for staff.

**Off Schedule 5 (Pricing Details)** Off Ref:

Crown Copyright 2018

## Call-Off Schedule 5 (Pricing Details)

**[Guidance Note:** This Schedule should be used to show further detailed pricing information, in addition to the pricing in the Order Form]



Framework Ref: RM6116

Project Version: v1.0 1

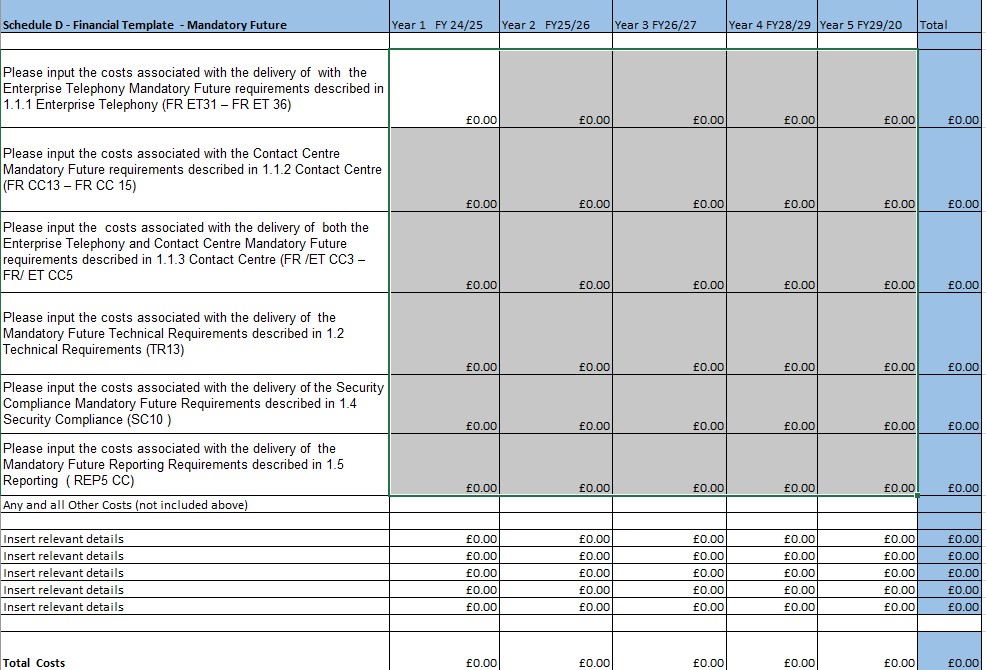


Table A provides the description of the services and related end user quantities which constitute the pricing.

### Table A

**Enetrprise Telephony**

|  |  |
| --- | --- |
| **Description** | **Quantity** |
| UCC Microsoft Teams - Direct Routing Service MS Teams Direct Routing | 182 |
| UCC Network Connectivity Service Customer Landing Zone | 1 |
| UCC Administration Service Self Service Portal | 1 |
| UCC Voice Services Service Voice - Premium | 3900 |
| Gamma PSTN Services Service PSTN - DDI | 3682 |
| Gamma PSTN Services Service PSTN - SIP Trunk Call Manager | 3682 |
| Tiger Reporting / Analytics Service Call Analytics | 3900 |

**Contact Centre**

|  |  |
| --- | --- |
| **Description** | **Quantity** |
| UCC Contact Centre Service Contact Centre | 1 |
| UCC Contact Centre Service Contatc Centre - Agent Multi Channel | 100 |
| UCC Contact Centre Service Contact Centre - CMS Port IVR Port | 20 |
| UCC Contact Centre Service Contact Centre - Manager | 11 |
| ASC Voice Recording Service Voice Recording - Premium - Contact Centre | 1 |
| ASC Voice Recording Service Voice Recording - Premium - Agent | 100 |
| ASC Voice Recording Service Voice Recording - Premium - Manager | 11 |
| Callabrio WFM | 100 |

**Desk Phones**

|  |  |
| --- | --- |
| **Description** | **Quantity** |
| Devices Power Adapter UK | 400 |
| OpenScape CP10 | 400 |
| OpenScape Desk Phone CP710 | 400 |
| Initial Disposal of phones | 300 |

**Soft Phone**

|  |  |
| --- | --- |
| **Description** | **Quantity** |
| Unify Phone | 3500 |

**Technical Configuration**

|  |  |
| --- | --- |
| **Description** | **Quantity** |
| WFM - Setup and Deployment | 1 |
| UCC Microsoft Teams - Direct Routing Setup and Deployment | 1 |
| Unify Phone Setup and Deployment | 1 |

**Non-functional requirement Cost**

|  |  |
| --- | --- |
| **Description** | **Quantity** |
| Not required in Unify solution | N/a |
| **Transition Cost** |  |
| **Description** | **Quantity** |
| Project Management | 1 |
| **Call-plan Charges** |  |
| **Description** | **Quantity** |
| Gamma PSTN Services Service PSTN - Bundled Minutes | 3682 |

**Training**

|  |  |
| --- | --- |
| **Description** | **Quantity** |
| WFM Training | 1 |
| Basic Unify Phone | 1 |

As the incumbent supplier of services today we do not anticipate the need to deliver training for all users in the HSE estate. This is the benefit of enhancing the existing solution rather than a rip and replace with new technology. However, we appreciate that there may be some pockets of users who will need refresher training and to allow the HSE to plan we have included the possible courses and corresponding daily rates in Table B. It should be noted that we have included pricing for training for the new services, WFM and Basic Unify Phone, in Schedule D, Mandatory Immediate – Training.

### Table B

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Course Name** | **Intended For** | **Duration** | **Max no.**  **Delegates &**  **Venue** | **Course price** |
| **Openscape Voice Administration training** | | | |  |
| OpenScape Solution  Basic  Administration 1 | For System Managers to be able to interrogate the system software, interpret command outputs and carry out moves and changes to the | 4 Days | Per delegate | £2,250.00 |
| Atos Nottingham | Per delegate |
| **OpenScape Contact Centre training** | | | |  |
| OpenScape Agent  Portal application - Key user or Train the Trainer approach \*\*\*Optional\*\*\* | This course is suitable for personnel who will be supporting Agents using the Agent Portal application. | 1 Day  (10 delegates per session x 2) | Max 20 delegates per  day | £850.00 |
| Customer premises or remote | per day |
| OpenScape Contact Center Real time &  Broadcaster  \*\*\*Optional\*\*\* | Call Center Managers, Supervisors and Team Leaders involved in the day to day management of the center. | 1 day | Max 8 delegates per day | £850.00 |
| Customer premises or remote | per day |
| OpenScape Contact Center Historical reports  \*\*\*Optional\*\*\* | Call Center Managers, Supervisors and Team Leaders involved in the day to day management of the center. | 1 day | Max 8 delegates per day | £850.00 |
| Customer premises or remote | per day |
| OpenScape Contact  Center Basic  Administration  **\*\*\*Optional\*\*\*** | Call Center Managers, Supervisors and Team  Leaders who will need to manage the application. | 1 day | Max 4 delegates per day | £1,000.00 |
| Customer premises or remote | per day |
| **Unify Teams direct routing training** | | | |  |
| MS Teams end user \*\*\*Optional\*\*\* | This course is suitable for personnel who will be supporting users of Teams. | 1 Day  10 delegates per session x 3 | Max 30 delegates per day | £850.00 |
| Customer premises | per day |
|  | | | |  |

## Call-Off Schedule 6 (ICT Services)

### 1. Definitions

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

|  |  |
| --- | --- |
| **"Buyer Property"** | the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract; |
| **"Buyer Software"** | any software which is owned by or licensed to the Buyer and which is or will be used by the  Supplier for the purposes of providing the Deliverables; |
| **"Buyer System"** | the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables; |
| **“Commercial off the shelf Software” or “COTS Software”**      **“Core Network”** | Non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms    the provision of any shared central core network capability forming part of the overall Services delivered to the Buyer, which is not specific or exclusive to a specific Call-Off Contract, and excludes any configuration information specifically associated with a specific Call-Off Contract; |
| **"Defect"** | any of the following:  a) any error, damage or defect in the manufacturing of a Deliverable; or |

|  |  |
| --- | --- |
|  | b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or |
|  | 1. any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or 2. any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract; |
| **"Emergency**  **Maintenance"** | ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault; |
| **"ICT Environment"** | the Buyer System and the Supplier System; |
| **"Licensed Software"** | all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software; |
| **"Maintenance**  **Schedule"** | has the meaning given to it in paragraph 8 of this Schedule; |
| **"Malicious Software"** | any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence; |

|  |  |
| --- | --- |
| **"New Release"** | an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item; |
| **"Open Source**  **Software"** | computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge; |
| **"Operating**  **Environment"** | means the Buyer System and any premises (including the Buyer Premises, the Supplier’s premises or third party premises) from, to or at which:   1. the Deliverables are (or are to be) provided; or 2. the Supplier manages, organises or otherwise directs the provision or the use of the   Deliverables; or   1. where any part of the Supplier System is situated; |
| **"Permitted**  **Maintenance"** | has the meaning given to it in paragraph 8.2 of this Schedule; |
| **"Quality Plans"** | has the meaning given to it in paragraph 6.1 of this Schedule; |
| **"Sites"** | has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the  Buyer System takes place; |
| **"Software"** | Specially Written Software COTS Software and non-COTS Supplier and third party Software; |
| **"Software Supporting**  **Materials"** | has the meaning given to it in paragraph 9.1 of this Schedule; |
| **"Source Code"** | computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction,  maintenance, modification and enhancement of such software; |
| **"Specially Written**  **Software"** | any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially  Written Software does not constitute New IPR; |
|  |  |
| **"Supplier System"** | the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System); |
|  |  |

### 2. When this Schedule should be used

2.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT Services which are part of the Deliverables.

### 3. Buyer due diligence requirements

3.1. This paragraph 3 applies where the Buyer has conducted a Further Competition Procedure. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;

3.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;

3.1.2. operating processes and procedures and the working methods of the Buyer;

3.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and

3.1.4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.

3.2. The Supplier confirms that it has advised the Buyer in writing of:

3.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;

3.2.2. each aspect, if any, of the Operating Environment where the provision of the Services will be subject to site surveys, wayleaves and/or any other consents not yet granted;

3.2.3. the actions needed to remedy each such unsuitable aspect; and

3.2.4. a timetable for and the costs of those actions.

### 4. Licensed software warranty

4.1. The Supplier represents and warrants that:

4.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any SubContractor) to the Buyer which are necessary for the performance of the Supplier’s obligations under this Contract including the receipt of the Deliverables by the Buyer;

4.1.2. all components of the Specially Written Software shall:

4.1.2.1. be free from material design and programming errors;

4.1.2.2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14

(Service Levels) and Documentation; and 4.1.2.3. not infringe any IPR.

### 5. Provision of ICT Services

5.1. The Supplier shall:

5.1.1. ensure that the release of any new COTS Software in which the

Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;

5.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;

5.1.3. ensure that the Supplier System will be free of all encumbrances;

5.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;

5.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

### 6. Standards and Quality Requirements

6.1. The Supplier shall where requested by the Buyer as part of their Further Competition Procedure, develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**")**.**

6.2. The Supplier shall seek Approval from the Buyer (not to be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.

6.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.

6.4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:

6.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;

6.4.2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and

6.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

### 7. ICT Audit

7.1. The Supplier shall allow any auditor access to the Supplier premises to:

7.1.1. inspect the ICT Environment and the wider service delivery environment (or any part of them);

7.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;

7.1.3. review the Supplier’s quality management systems including all relevant Quality Plans.

### 8. Maintenance of the ICT Environment

8.1. If requested by the Buyer as part of its Further Competition Procedure, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.

8.2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (other than to the Core Network) (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.

8.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance, including to the Core Network.

8.4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

### 9. Intellectual Property Rights in ICT

#### 9.1. Assignments granted by the Supplier: Specially Written Software

9.1.1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:

9.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and

9.1.1.2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").

9.1.2. The Supplier shall:

9.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;

9.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source

Code and Object Code forms together with relevant

Documentation and all related Software Supporting

Materials within seven days of completion or, if a relevant

Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and

9.1.2.3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier’s Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royaltyfree licence to use, sub-license and/or commercially exploit such Supplier’s Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

9.1.3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

9.2. **Licences for non-COTS IPR from the Supplier and third parties to the**

### Buyer

9.2.1. Unless the Buyer gives its Approval the Supplier must not use any:

1. of its own Existing IPR that is not COTS Software;
2. third party software that is not COTS Software

9.2.2. Where the Buyer Approves the use of the Supplier’s Existing IPR that is not COTS Software the Supplier shall grant to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer’s (or, if the Buyer is a Central Government Body, any other Central Government Body’s) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Call Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

9.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to

the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

9.2.3.1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and

9.2.3.2. only use such third party IPR as referred to at paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

9.2.4. Where the Supplier is unable to provide a license to the Supplier’s Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

9.2.5. The Supplier may terminate a licence granted under paragraph 9.2.1 by giving at least thirty (30) days’ notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

9.3. **Licenses for COTS Software by the Supplier and third parties to the**

### Buyer

9.3.1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licencee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:

9.3.4.1. will no longer be maintained or supported by the developer; or

9.3.4.2. will no longer be made commercially available

#### 9.4. Buyer’s right to assign/novate licences

9.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 9.2 (to:

9.4.1.1. a Central Government Body; or

9.4.1.2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.

9.4.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 9.2.

#### 9.5. Licence granted by the Buyer

9.5.1. The Buyer grants to the Supplier a royalty-free, non-exclusive, nontransferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).

#### 9.6. Open Source Publication

9.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

9.6.1.1. suitable for publication by the Buyer as Open Source; and

9.6.1.2. based on Open Standards (where applicable), and the Buyer may, at its sole discretion, publish the same as Open Source.

9.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:

9.6.2.1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;

9.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;

9.6.2.3. do not contain any material which would bring the Buyer into disrepute;

9.6.2.4. can be published as Open Source without breaching the rights of any third party;

9.6.2.5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and

9.6.2.6. do not contain any Malicious Software.

9.6.3. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:

9.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and

9.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer’s ability to publish such other items or Deliverables as Open Source.

#### 9.7. Malicious Software

9.7.1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.

9.7.2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.

9.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.7.2 shall be borne by the Parties as follows:

9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious

Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

9.7.3.2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

#### 10. [Supplier-Furnished Terms

##### 10.1. Software Licence Terms

10.1.1. Terms for licensing of non-COTS third party software in accordance with Paragraph 9.2.3 are detailed in Part 1A of Call Off Schedule 24 (Supplier Furnished Terms)

10.1.2. Terms for licensing of COTS software in accordance with

Paragraph 9.3 are detailed in Part 1B of Call Off Schedule 24 (Supplier Furnished Terms)

### i) 11. Customer Premises

#### 11.1. Licence to occupy Buyer Premises

11.1.1. Any Buyer Premises shall be made available to the Supplier on a non-exclusive licence basis free of charge and shall be used by the Supplier solely for the purpose of performing its obligations under this Call-Off Contract. The Supplier shall have the use of such Buyer Premises as licensee and shall vacate the same immediately upon completion, termination, expiry or abandonment of this Call-Off Contract and in accordance with Call-Off Schedule 10 (Exit Management).

11.1.2 The Supplier shall limit access to the Buyer Premises to such Supplier Staff as is necessary to enable it to perform its obligations under this Call-Off Contract and the Supplier shall co-operate (and ensure that the Supplier Staff co-operate) with such other persons working concurrently on such Buyer Premises as the Buyer may reasonably request.

11.1.3 Save in relation to such actions identified by the Supplier in accordance with paragraph 3.2 of this Call-Off Schedule 6 and set out in the Order Form (or elsewhere in this Call-Off Contract), should the Supplier require modifications to the Buyer Premises, such modifications shall be subject to Approval and shall be carried out by the Buyer at the Supplier's expense. The Buyer shall undertake any modification work which it approves pursuant to this paragraph 11.1.3 without undue delay. Ownership of such modifications shall rest with the Buyer.

11.1.4 The Supplier shall observe and comply with such rules and regulations as may be in force at any time for the use of such Buyer Premises and conduct of personnel at the Buyer Premises as determined by the Buyer, and the Supplier shall pay for the full cost of making good any damage caused by the Supplier Staff other than fair

wear and tear. For the avoidance of doubt, damage includes without limitation damage to the fabric of the buildings, plant, fixed equipment or fittings therein.

11.1.5 The Parties agree that there is no intention on the part of the

Buyer to create a tenancy of any nature whatsoever in favour of the Supplier or the Supplier Staff and that no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to this Call-Off Contract, the Buyer retains the right at any time to use any Buyer Premises in any manner it sees fit.

#### 11.2. Security of Buyer Premises

11.2.1 The Buyer shall be responsible for maintaining the security of the Buyer Premises. The Supplier shall comply with the reasonable security requirements of the Buyer while on the Buyer Premises.

11.2.2 The Buyer shall afford the Supplier upon Approval (the decision to Approve or not will not be unreasonably withheld or delayed) an opportunity to inspect its physical security arrangements.

#### 12. Buyer Property

12.1. Where the Buyer issues Buyer Property free of charge to the

Supplier such Buyer Property shall be and remain the property of the Buyer and the Supplier irrevocably licences the Buyer and its agents to enter upon any premises of the Supplier during normal business hours on reasonable notice to recover any such Buyer Property.

12.2. The Supplier shall not in any circumstances have a lien or any other interest on the Buyer Property and at all times the Supplier shall possess the Buyer Property as fiduciary agent and bailee of the Buyer.

12.3. The Supplier shall take all reasonable steps to ensure that the title of the Buyer to the Buyer Property and the exclusion of any such lien or other interest are brought to the notice of all Subcontractors and other appropriate persons and shall, at the Buyer's request, store the Buyer Property separately and securely and ensure that it is clearly identifiable as belonging to the Buyer.

12.4. The Buyer Property shall be deemed to be in good condition when received by or on behalf of the Supplier unless the Supplier notifies the Buyer otherwise within five (5) Working Days of receipt.

12.5. The Supplier shall maintain the Buyer Property in good order and condition (excluding fair wear and tear) and shall use the Buyer Property solely in connection with this Call-Off Contract and for no other purpose without Approval.

12.6. The Supplier shall ensure the security of all the Buyer Property whilst in its possession, either on the Sites or elsewhere during the supply of the Services, in accordance with Call-Off Schedule 9 (Security) and the Buyer’s reasonable security requirements from time to time.

12.7. The Supplier shall be liable for all loss of, or damage to the Buyer Property, (excluding fair wear and tear), unless such loss or damage was solely caused by an Authority Cause. The Supplier shall inform the Buyer immediately of becoming aware of any defects appearing in or losses or damage occurring to the Buyer Property.

#### 13. Supplier Equipment

13.1. Unless otherwise stated in the Order Form (or elsewhere in this Call-Off Contract), the Supplier shall provide all the Supplier Equipment necessary for the provision of the Services.

13.2. The Supplier shall not deliver any Supplier Equipment nor begin any work on the Buyer Premises without obtaining Approval.

13.3. The Supplier shall be solely responsible for the cost of carriage of the Supplier Equipment to the Sites and/or any Buyer Premises, including its off-loading, removal of all packaging and all other associated costs. Likewise on the Call-Off Expiry Date the Supplier shall be responsible for the removal of all relevant Supplier Equipment from the Sites and/or any Buyer Premises, including the cost of packing, carriage and making good the Sites and/or the Buyer Premises following removal.

13.4. All the Supplier's property, including Supplier Equipment, shall remain at the sole risk and responsibility of the Supplier, except that the Buyer shall be liable for loss of or damage to any of the Supplier's property located on Buyer Premises which is due to the negligent act or omission of the Buyer.

13.5. Subject to any express provision of the BCDR Plan (if applicable) to the contrary, the loss or destruction for any reason of any Supplier Equipment shall not relieve the Supplier of its obligation to supply the Services in accordance with this Call Off Contract, including the Service Levels.

13.6. The Supplier shall maintain all Supplier Equipment within the Sites and/or the Buyer Premises in a safe, serviceable and clean condition.

13.7. The Supplier shall, at the Buyer’s written request, at its own expense and as soon as reasonably practicable:

13.7.1. remove from the Buyer Premises any Supplier Equipment or any component part of Supplier Equipment which in the reasonable opinion of the Buyer is either hazardous, noxious or not in accordance with this Call-Off Contract; and

13.7.2. replace such Supplier Equipment or component part of Supplier Equipment with a suitable substitute item of Supplier Equipment.

Call-Off Schedule 7 (Key Supplier Staff) Call-Off Ref:

Crown Copyright 2018

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

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

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

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

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

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

1.4.2 the person concerned resigns, retires or dies or is on maternity or longterm 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

Framework Ref: RM6116

Project Version: v1.0 1

1

Call-Off Schedule 7 (Key Supplier Staff) Call-Off Ref:

Crown Copyright 2018

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.

Framework Ref: RM6116

Project Version: v1.0 2

1

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

### 1. Definitions

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

|  |  |
| --- | --- |
| **“Annual Revenue”** | means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology:   1. figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and 2. where the Supplier, the Supplier Group and/or their joint ventures and   Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date; |
| **“Appropriate Authority”**  **or “Appropriate Authorities”** | means the Buyer and the Cabinet Office Markets and Suppliers Team or, where the  Supplier is a Strategic Supplier, the Cabinet  Office Markets and Suppliers Team; |
| **“Associates”** | means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles; |
| **"BCDR Plan"** |  |

|  |  |
| --- | --- |
|  | a plan which details the processes and arrangements that the Supplier shall follow to:   1. ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and 2. the recovery of the Deliverables in the event of a Disaster; |
| **"Business Continuity**  **Plan"** | has the meaning given to it in Paragraph  1.3.2 of this Schedule; |
| **“Class 1 Transaction”** | has the meaning set out in the listing rules issued by the UK Listing Authority; |
| **“Control”** | the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “**Controls**” and “**Controlled**” shall be interpreted accordingly; |
| **“Corporate Change**  **Event”** | means:   1. any change of Control of the Supplier or a Parent Undertaking of the Supplier; 2. any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Deliverables; 3. any change to the business of the   Supplier or any member of the Supplier  Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Deliverables;   1. a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the   London Stock Exchange plc;   1. an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the   Supplier or any Parent Undertaking of the Supplier; |

|  |  |
| --- | --- |
|  | (f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net  Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period; (g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;   1. any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group; 2. the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the   Supplier Group; and/or   1. any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the   Supplier Group in a jurisdiction outside  England and Wales; |
| **“Critical National**  **Infrastructure”** | means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:   1. major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or 2. significant impact on the national security, national defence, or the functioning of the UK; |

|  |  |
| --- | --- |
| **“Critical Service**  **Contract”** | a service contract which the Buyer has categorised as a Gold Contract using the Cabinet Office Contract Tiering Tool or which the Buyer otherwise considers should be classed as a Critical Service Contract; |
| **“CRP Information”** | means, together, the:  Group Structure Information and Resolution Commentary; and  UK Public Sector and CNI Contract Information; |
| **“Dependent Parent**  **Undertaking”** | means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into the Contract, including for the avoidance of doubt the provision of the Deliverables in accordance with the terms of the Contract; |
| **"Disaster"** | the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable); |
| **"Disaster Recovery**  **Deliverables"** | the Deliverables embodied in the processes and procedures for restoring the provision of  Deliverables following the occurrence of a Disaster; |
| **"Disaster Recovery Plan"** | has the meaning given to it in Paragraph  1.3.3 of this Schedule; |
| **"Disaster Recovery**  **System"** | the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster; |
| **“Group Structure**  **Information and**  **Resolution Commentary”** | means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 to 4 and Appendix 1 to Part C; |
| **“Parent Undertaking”** | has the meaning set out in section 1162 of the Companies Act 2006; |
| **“Public Sector Dependent**  **Supplier”** | means a supplier where that supplier, or that supplier’s group has Annual Revenue of £50 million or more of which over 50% is generated from UK Public Sector Business; |
| **"Related Supplier"** | any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time; |
| **"Review Report"** | has the meaning given to it in Paragraph 6.3 of Part B of this Schedule; |
| **“Strategic Supplier”** | means those suppliers to government listed at  https://www.gov.uk/government/publications/ strategic-suppliers; |
| **“Subsidiary Undertaking”** | has the meaning set out in section 1162 of the Companies Act 2006; |
| **“Supplier Group”** | means the Supplier, its Dependent Parent  Undertakings and all Subsidiary  Undertakings and Associates of such  Dependent Parent Undertakings; |
| **"Supplier's Proposals"** | has the meaning given to it in Paragraph 6.3 of Part B of this Schedule; |
| **“UK Public Sector**  **Business”** | means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, nondepartmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations; and |
| **“UK Public Sector / CNI**  **Contract Information”** | means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 to 4 of Part C and Appendix 2 of Part C; |

### Part A: BCDR Plan

**Unless otherwise specified in this Schedule, this Part A shall apply only to Call-Off Contracts which have been awarded via Direct Award in accordance with Framework Schedule 7 (Call-Off Contract Award Procedure).**

[**Buyer Guidance:** This Part A should not be deleted from any Call-Off Contracts as it interacts with Part B in certain circumstances].

#### 1. BCDR Plan

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

1.2 Promptly (and in any event within 30 days) after the Start Date, the Supplier shall provide to the Buyer its BCDR Plan.

1.3 The Supplier shall ensure at all times that its BCDR Plan conforms with Good Industry Practice.

1.4 The Supplier may from time to time during the Contract Period review, update, and/or test its BCDR Plan. The Supplier shall ensure that any use by it or any Subcontractor of "live" buyer 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.

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

1.5.1 the outcome of the test;

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

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

1.6 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke its 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.

1.7 To the extent the BCDR Plan contains processes, procedures, and/or other content which is designed to permit the continuity of the business operations of the Buyer supported by the Deliverables through continued provision of the Deliverables following an Insolvency Event of the Supplier, any Key Subcontractor and/or any supplier, the BCDR Plan shall be invoked by the Supplier:

where an Insolvency Event of a Key Sub-contractor and/or Supplier Group member (other than the Supplier) could reasonably be expected to adversely affect delivery of the Deliverables; and/or where there is an Insolvency Event of the Supplier and the insolvency arrangements enable the Supplier to invoke the plan.

### Part B: BCDR Plan - Long Form

This Part B shall apply to all Call-Off Contracts which have been awarded via a

Further Competition procedure in accordance with Framework Schedule 7 (Call-Off Contract Award Procedure) and shall not apply to any Call-Off Contracts awarded via Direct Award.

#### 1. BCDR Plan

1.1 At least ninety (90) Working Days prior to the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer’s written approval a plan (a **“BCDR Plan”**), which shall detail the processes and arrangements that the Supplier shall follow to:

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

1.1.2 the recovery of the Deliverables in the event of a Disaster

1.2 The BCDR Plan shall be divided into four sections:

1.2.1 Section 1 which shall set out general principles applicable to the BCDR Plan

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

1.2.3 Section 3 which shall relate to disaster recovery (the **"Disaster**

**Recovery Plan"**); and1.2.4 Section 4 which shall relate to an Insolvency Event of the Supplier, and Key-Subcontractors and/or any Supplier Group member (the “**Insolvency Continuity Plan**”).

1.3 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.

1.4 To the extent the Supplier fails to supply its BCDR Plan in compliance with paragraph 1.2, the Buyer may at its discretion require the Supplier to promptly provide its BCDR Plan and comply with the provisions of Part A of this Schedule until the Supplier provides its BCDR Plan. Exercise by the Buyer of its rights under this paragraph 1.5 shall not prevent and/or restrict the Buyer from exercising its other rights and remedies under this Contract, and shall not relieve the Supplier of its obligations under this Part B.]

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

2.1 Section 1 of the BCDR Plan shall:

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

2.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;

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

2.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any Related Supplier(s) in each case as notified to the Supplier by the Buyer from time to time;

2.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

2.1.6 contain a risk analysis, including:

1. failure or disruption scenarios and assessments of likely frequency of occurrence;
2. identification of any single points of failure within the provision of

Deliverables and processes for managing those risks;

1. identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and
2. a business impact analysis of different anticipated failures or disruptions;

2.1.7 provide for documentation of processes, including business processes, and procedures;

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

2.1.9 identify the procedures for reverting to "normal service";

2.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;

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

2.1.12 provide for the provision of technical assistance to key contacts at the

Buyer as required by the Buyer to inform decisions in support of the Buyer’s business continuity plans;

2.1.13 set out how the business continuity and disaster recovery elements of the BCDR Plan link to the Insolvency Continuity Plan, and how the Insolvency Continuity Plan links to the business continuity and disaster recovery elements of the BCDR Plan;

2.1.14 contain an obligation upon the Supplier to liaise with the Buyer and (at the Buyer’s request) any Related Supplier with respect to issues concerning insolvency continuity where applicable; and

2.1.15 detail how the BCDR Plan links and interoperates with any overarching and/or connected insolvency continuity plan of the Buyer and any of its other Related Suppliers in each case as notified to the Supplier by the Buyer from time to time.

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

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

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

2.2.3 it complies with the relevant provisions of ISO/IEC 27002;

ISO22301/ISO22313 and all other industry standards from time to time in force; and

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

2.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.

2.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI’s) or Service levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

#### 3. Business Continuity (Section 2)

3.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:

3.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and

3.1.2 the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.

3.2 The Business Continuity Plan shall:

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

3.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;

3.2.3 specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI’s) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and

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

#### 4. Disaster Recovery (Section 3)

4.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

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

4.2.1 loss of access to the Buyer Premises;

4.2.2 loss of utilities to the Buyer Premises;

4.2.3 loss of the Supplier's helpdesk or CAFM system;

4.2.4 loss of a Subcontractor;

4.2.5 emergency notification and escalation process;

4.2.6 contact lists;

4.2.7 staff training and awareness;

4.2.8 BCDR Plan testing;

4.2.9 post implementation review process;

4.2.10 any applicable Performance Indicators (PI’s) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI’s) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;

4.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

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

4.2.13 testing and management arrangements.

#### 5. Insolvency Continuity Plan (Section 4)

5.1 The Insolvency Continuity Plan shall be designed by the Supplier to permit continuity of the business operations of the Buyer supported by the Deliverables through continued provision of the Deliverables following an Insolvency Event of the Supplier, any Key Sub-contractor and/or any Supplier Group member with, as far as reasonably possible, minimal adverse impact.

5.2 The Insolvency Continuity Plan shall include the following:

5.2.1 communication strategies which are designed to minimise the potential disruption to the provision of the Deliverables, including key contact details in respect of the supply chain and key contact details for operational and contract Supplier Staff, Key Subcontractor personnel and Supplier Group member personnel;

5.2.2 identification, explanation, assessment and an impact analysis of risks in respect of dependencies between the Supplier, Key Subcontractors and Supplier Group members where failure of those dependencies could reasonably have an adverse impact on the Deliverables;

5.2.3 plans to manage and mitigate identified risks;

5.2.4 details of the roles and responsibilities of the Supplier, Key Subcontractors and/or Supplier Group members to minimise and mitigate the effects of an Insolvency Event of such persons on the Deliverables;

5.2.5 details of the recovery team to be put in place by the Supplier (which may include representatives of the Supplier, Key Subcontractors and Supplier Group members); and

5.2.6 sufficient detail to enable an appointed insolvency practitioner to invoke the plan in the event of an Insolvency Event of the Supplier.

#### 6. Review and changing the BCDR Plan

6.1 The Supplier shall review the BCDR Plan:

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

6.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 8 of Part B; and

6.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of Part B 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.

6.2 Each review of the BCDR Plan pursuant to Paragraph 6.1 of Part B 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.

6.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

6.4 Following receipt of the Review Report and the Supplier’s Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier’s expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

#### 7. Testing the BCDR Plan

7.1 The Supplier shall test the BCDR Plan:

7.1.1 regularly and in any event not less than once in every Contract Year; 7.1.2 in the event of any major reconfiguration of the Deliverables

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

7.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer’s requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

7.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.

7.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.

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

7.5.1 the outcome of the test;

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

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

7.6 Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

#### 8. Invoking the BCDR Plan

8.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

8.2 The Insolvency Continuity Plan element of the BCDR Plan, including any linked elements in other parts of the BCDR Plan, shall be invoked by the Supplier:

8.2.1 where an Insolvency Event of a Key Sub-contractor and/or Supplier Group member (other than the Supplier) could reasonably be expected to adversely affect delivery of the Deliverables; and/or

8.2.2 where there is an Insolvency Event of the Supplier and the insolvency arrangements enable the Supplier to invoke the plan.

#### 9. Circumstances beyond your control

9.1 The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.

#### 10. Amendments to this Schedule in respect of Bronze Contracts

10.1 Where a Buyer’s Call-Off Contract is a Bronze Contract, if specified in the Order Form, the following provisions of this Call-Off Schedule 8, shall be disapplied in respect of that Contract:

10.1.1 Paragraph 1.3.4 of Part B so that the BCDR plan shall only be required to be split into the three sections detailed in paragraphs 1.3.1 to 1.3.3 of Part B inclusive;

10.1.2 Paragraphs 2.1.13 to 2.1.15 of Part B, inclusive;

10.1.3 Paragraph 5 (Insolvency Continuity Plan) of Part B;

10.1.4 Paragraph 8.2 of Part B; and

10.1.5 The entirety of Part C of this Schedule.

10.2 Where a Buyer’s Call-Off Contract is a Bronze Contract, if specified in the Order Form, the following definitions in Paragraph 1 of this Call-Off Schedule 8, shall be deemed to be deleted:

10.2.1 Annual Review;

10.2.2 Appropriate Authority or Appropriate Authorities;

10.2.3 Associates;

10.2.4 Class 1 Transaction;

10.2.5 Control;

10.2.6 Corporate Change Event;

10.2.7 Critical National Infrastructure;

10.2.8 Critical Service Contract;

10.2.9 CRP Information;

10.2.10 Dependent Parent Undertaking;

10.2.11 Group Structure Information and Resolution Commentary;

10.2.12 Parent Undertaking;

10.2.13 Public Sector Dependent Supplier;

10.2.14 Subsidiary Undertaking;

10.2.15 Supplier Group;

10.2.16 UK Public Sector Business; and

10.2.17 UK Public Sector/CNI Contract Information.

### Part C: Corporate Resolution Planning

#### 1. Service Status and Supplier Status

1.1 This Contract [insert ‘is’ or ‘is not’] a Critical Service Contract.

1.2 The Supplier shall notify the Buyer in writing within 5 Working Days of the Effective Date and throughout the Call-Off Contract Period within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier.

#### 2. Provision of Corporate Resolution Planning Information

2.1 Paragraphs 2 to 4 of this Part C shall apply if the Contract has been specified as a Critical Service Contract under Paragraph 1.1 of this Part C or the Supplier is or becomes a Public Sector Dependent Supplier.

2.2 Subject to Paragraphs 2.6, 2.10 and 2.11 of this Part C:

2.2.1 where the Contract is a Critical Service Contract, the Supplier shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the Effective Date; and

2.2.2 except where it has already been provided, where the Supplier is a

Public Sector Dependent Supplier, it shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the date of the Appropriate Authority’s or Appropriate Authorities’ request.

2.3 The Supplier shall ensure that the CRP Information provided pursuant to Paragraphs 2.2, 2.8 and 2.9 of this Part B:

2.3.1 is full, comprehensive, accurate and up to date;

2.3.2 is split into two parts:

1. Group Structure Information and Resolution Commentary;
2. UK Public Service / CNI Contract Information and is structured and presented in accordance with the requirements and explanatory notes set out at Annex I of the latest published version of the Resolution Planning Guidance published by the Cabinet Office Government Commercial Function and available at

https://www.gov.uk/government/publications/the-

outsourcingplaybook and contains the level of detail required

(adapted as necessary to the Supplier’s circumstances);

2.3.3 incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Appropriate Authority or Appropriate Authorities to understand and consider the information for approval;

2.3.4 provides a clear description and explanation of the Supplier Group members that have agreements for goods, services or works provision

in respect of UK Public Sector Business and/or Critical National Infrastructure and the nature of those agreements; and

2.3.5 complies with the requirements set out at Appendix 1 (Group Structure Information and Resolution Commentary) and Appendix 2 (UK Public Sector / CNI Contract Information) respectively.

2.4 Following receipt by the Appropriate Authority or Appropriate Authorities of the CRP Information pursuant to Paragraphs 2.2, 2.8 and 2.9 of this Part C, the Buyer shall procure that the Appropriate Authority or Appropriate Authorities shall discuss in good faith the contents of the CRP Information with the Supplier and no later than 60 days after the date on which the CRP Information was delivered by the Supplier either provide an Assurance to the Supplier that the Appropriate Authority or Appropriate Authorities approves the CRP Information or that the Appropriate Authority or Appropriate Authorities rejects the CRP Information.

2.5 If the Appropriate Authority or Appropriate Authorities rejects the CRP Information:

2.5.1 the Buyer shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Supplier in writing of its reasons for its rejection; and

2.5.2 the Supplier shall revise the CRP Information, taking reasonable account of the Appropriate Authority’s or Appropriate Authorities’ comments, and shall re-submit the CRP Information to the Appropriate Authority or Appropriate Authorities for approval within 30 days of the date of the Appropriate Authority’s or Appropriate Authorities’ rejection. The provisions of paragraph 2.3 to 2.5 of this Part C shall apply again to any resubmitted CRP Information provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure under Clause 34 of the Core Terms at any time.

2.6 Where the Supplier or a member of the Supplier Group has already provided CRP Information to a Department or the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that Department and the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid (which has the meaning in paragraph 2.7 below) on the date by which the CRP Information would otherwise be required, the Supplier shall not be required to provide the CRP Information under Paragraph 2.2 of this Part C if it provides a copy of the Valid Assurance to the Appropriate Authority or Appropriate Authorities on or before the date on which the CRP Information would otherwise have been required.

2.7 An Assurance shall be deemed Valid for the purposes of Paragraph 2.6 of this Part C if:

2.7.1 the Assurance is within the validity period stated in the Assurance (or, if no validity period is stated, no more than 12 months has elapsed since

it was issued and no more than 18 months has elapsed since the Accounting Reference Date on which the CRP Information was based); and

2.7.2 no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if the Contract had then been in force) have occurred since the date of issue of the Assurance.

2.8 If the Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 2.8.3 of this Part C its initial CRP Information) to the Appropriate Authority or Appropriate Authorities:

2.8.1 within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 2.11 of this Part C) unless the Supplier is relieved of the consequences of the Financial Distress Event under Paragraph 7.1 of Joint Schedule 7 (Financial Distress) (if applicable);

2.8.2 within 30 days of a Corporate Change Event unless not required pursuant to Paragraph 2.10 of this Part C;

2.8.3 within 30 days of the date that:

1. the credit rating(s) of each of the Supplier and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 2.10 of this Part C; or
2. none of the credit rating agencies specified at Paragraph 2.10 of this Part C hold a public credit rating for the Supplier or any of its Parent Undertakings; and

2.8.4 in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Appropriate Authority (whichever is the earlier), unless:

1. updated CRP Information has been provided under any of Paragraphs 2.8.1 2.8.2 or 2.8.3 of this Part C since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 2.8.4; or
2. unless not required pursuant to Paragraph 2.10 of this Part C.
   1. Where the Supplier is a Public Sector Dependent Supplier and the Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 2.8.1 to 2.8.4 of this Part C, the Supplier shall provide at the request of the Appropriate Authority or Appropriate Authorities and within the applicable timescales for each event as set out in Paragraph 2.8 (or such longer timescales as may be notified to the Supplier by the Buyer), the CRP Information to the Appropriate Authority or Appropriate Authorities.
   2. Where the Supplier or a Parent Undertaking of the Supplier has a credit rating of either:
      1. Aa3 or better from Moody’s;
      2. AA- or better from Standard and Poors; 2.10.3 AA- or better from Fitch; the Supplier will not be required to provide any CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Supplier is relieved of the consequences of the Financial Distress Event under Paragraph 7.1 of Annex 3 to Joint Schedule 7 (Financial Distress), if applicable) or (ii) the

Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 2.10 of this Part C, in which cases the Supplier shall provide the updated version of the CRP Information in accordance with paragraph 2.8 of this Part C.

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

#### 3. Termination Rights

3.1 The Buyer shall be entitled to terminate the Contract if the Supplier is required to provide CRP Information under Paragraph 2 of this Part C and either:

3.1.1 the Supplier fails to provide the CRP Information within 4 months of the Effective Date if this is a Critical Service Contract or otherwise within 4 months of the Appropriate Authority’s or Appropriate Authorities’ request; or

3.1.2 the Supplier fails to obtain an Assurance from the Appropriate Authority or Appropriate Authorities within 4 months of the date that it was first required to provide the CRP Information under the Contract,

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

#### 4. Confidentiality and usage of CRP Information

4.1 The Buyer agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Supplier and/or Supplier Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality.

4.2 Where the Appropriate Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier’s request, the Buyer shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Supplier containing terms no less stringent than those placed on the Buyer under paragraph 4.1 of this Part C and Clause 15 of the Core Terms.

4.3 The Supplier shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Appropriate Authority or Appropriate Authorities pursuant to Paragraph 2 of this Part C subject, where necessary, to the Appropriate Authority or Appropriate Authorities entering into an appropriate confidentiality agreement in the form required by the third party.

4.4 Where the Supplier is unable to procure consent pursuant to Paragraph 4.3 of this Part C, the Supplier shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by:

4.4.1 redacting only those parts of the information which are subject to such obligations of confidentiality;

4.4.2 providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:

1. summarising the information;
2. grouping the information;
3. anonymising the information; and
4. presenting the information in general terms

4.5 The Supplier shall provide the Appropriate Authority or Appropriate Authorities with contact details of any third party which has not provided consent to disclose CRP Information where that third party is also a public sector body and where the Supplier is legally permitted to do so.

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

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

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

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

## Call-Off Schedule 9 (Security)

**[Guidance Note:** Buyer to Select whether or when Part A (Short Form Security Requirements) or Part B (Long Form Security Requirements) should apply. Part B should be considered where there is a high level of risk to personal or sensitive data.]

## Part A: Short Form Security Requirements

### 1. Definitions

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

|  |  |
| --- | --- |
| **"Breach of Security"** | **the occurrence of:**   1. **any unauthorised access to or use of the**   **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**   1. **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,**  **in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;** |
| **"Security**  **Management Plan"** | **the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.** |

### 2. Complying with security requirements and updates to them

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

2.2 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

2.3 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

2.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

2.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

### 3. Security Standards

3.1 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 security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

3.2.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.

3.3 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

### 4. Security Management Plan

#### 4.1 Introduction

4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

#### 4.2 Content of the Security Management Plan

4.2.1 The Security Management Plan shall:

1. comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;
2. identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
3. detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites 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;

1. 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, 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;

1. 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 provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the

Deliverables comply with the provisions of this Contract;

1. set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and
2. be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

#### 4.3 Development of the Security Management Plan

4.3.1 Within twenty (20)Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph

4.3.2. However a refusal by the Buyer 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.

4.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

#### 4.4 Amendment of the Security Management Plan

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

1. emerging changes in Good Industry Practice;
2. any change or proposed change to the Deliverables and/or associated processes;
3. where necessary in accordance with paragraph 2.2, any change to the Security Policy;
4. any new perceived or changed security threats; and
5. any reasonable change in requirements requested by the Buyer.

4.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and

amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation: a) suggested improvements to the effectiveness of the Security

Management Plan;

* 1. updates to the risk assessments; and
  2. suggested improvements in measuring the effectiveness of controls.
     1. Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.
     2. The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

### 5. Security breach

5.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

5.2.1 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 to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted

Breach of Security;

1. prevent an equivalent breach in the future exploiting the same cause failure; and
2. as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or

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

5.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

## Part B: Long Form Security Requirements

### 1. Definitions

1.1 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:**   1. **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** 2. **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,**  **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.** |

### 2. Security Requirements

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

2.2 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.

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

2.3.1 [insert security representative of the Buyer]

2.3.2 [insert security representative of the Supplier]

2.4 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.

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

2.6 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.

2.7 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.

2.8 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.

### 3. Information Security Management System (ISMS)

3.1 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.

3.2 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.

3.3 The Buyer acknowledges that;

3.3.1 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

3.3.2 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.

3.4 The ISMS shall:

3.4.1 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;

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

3.4.3 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/securitypolicy-framework/hmg-security-policy-framework)](https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework)

1. takes account of guidance issued by the Centre for

Protection of National Infrastructure

[(https://www.cpni.gov.uk)](https://www.cpni.gov.uk/)

1. complies with HMG Information Assurance Maturity

Model and Assurance Framework

[(https://www.ncsc.gov.uk/articles/hmg-ia-maturity-modeliamm)](https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm)

1. meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;
2. addresses issues of incompatibility with the Supplier’s own organisational security policies; and
3. complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.4 document the security incident management processes and incident response plans;

3.4.5 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

3.4.6 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).

3.5 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.

3.6 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.

3.7 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.

3.8 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.

### 4. Security Management Plan

4.1 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.

4.2 The Security Management Plan shall:

4.2.1 be based on the initial Security Management Plan set out in Annex 2

(Security Management Plan);

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

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

4.2.4 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;

4.2.5 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;

4.2.6 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);

4.2.7 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);

4.2.8 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;

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

4.2.10 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

4.2.11 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.

4.3 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 nonapproval 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.

4.4 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.

### 5. Amendment of the ISMS and Security Management Plan

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

5.1.1 emerging changes in Good Industry Practice;

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

5.1.3 any new perceived or changed security threats;

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

5.1.5 any new perceived or changed security threats; and

5.1.6 any reasonable change in requirement requested by the Buyer.

5.2 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:

5.2.1 suggested improvements to the effectiveness of the ISMS;

5.2.2 updates to the risk assessments;

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

5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 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.

5.4 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.

### 6. Security Testing

6.1 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.

6.2 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.

6.3 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 underperformance for the period of the Buyer’s test.

6.4 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 unpatched 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.

6.5 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.

### 7. Complying with the ISMS

7.1 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.

7.2 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.

7.3 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.

### 8. Security Breach

8.1 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.

8.2 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:

8.2.1 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;

1. 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;

1. prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and
2. 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
3. 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.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the 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.

### 9. Vulnerabilities and fixing them

9.1 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.

9.2 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: 9.2.1 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

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

9.3 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:

9.3.1 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;

9.3.2 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

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

9.4 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:

9.4.1 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

9.4.2 is agreed with the Buyer in writing.

9.5 The Supplier shall:

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

9.5.2 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;

9.5.3 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;

9.5.4 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;

9.5.5 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;

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

9.5.7 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

9.5.8 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.

9.6 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.

9.7 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

### 1. Handling Classified information

1.1 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.

### 2. End user devices

2.1 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.

2.2 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/enduser-device-security)](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.

### 3. Data Processing, Storage, Management and Destruction

3.1 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.

3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

3.3 The Supplier shall:

3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

### 4. Ensuring secure communications

4.1 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.

4.2 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.

### 5. Security by design

5.1 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.

5.2 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)](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).

### 6. Security of Supplier Staff

6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

### 7. Restricting and monitoring access

7.1 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.

### 8. Audit

8.1 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:

8.1.1 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.

8.1.2 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.

8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

## Part B – Annex 2 - Security Management Plan

[ ]

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

#### 1. Definitions

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

|  |  |
| --- | --- |
| “Core Network” | the provision of any shared central core network capability forming part of the overall Services delivered to the Buyer, which is not specific or exclusive to a specific Call-Off Contract, and excludes any configuration information specifically associated with a specific Call-Off Contract; |
| “Core Network Assets” | the assets used in the provision of the Core Network; |
| **"Exclusive Assets"** | Supplier Assets used exclusively by the Supplier [or a Key Subcontractor] in the provision of the Deliverables; |
| **"Exit Information"** | has the meaning given to it in Paragraph 3.1 of this Schedule; |
| **"Exit Manager"** | the person appointed by each Party to manage their respective obligations under this Schedule; |
| **“Exit Plan”** | the plan produced and updated by the Supplier during the Initial Period in accordance with Paragraph 4 of this Schedule; |
| **"Net Book Value"** | the current net book value of the relevant Supplier Asset(s) calculated in  accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice); |
| **"Non-Exclusive Assets"** | those Supplier Assets used by the Supplier [or a Key Subcontractor] in connection with the Deliverables but which are also used by the Supplier [or Key Subcontractor] for other purposes excluding the Core Network Assets; |

|  |  |
| --- | --- |
| **"Registers"** | the register and configuration database referred to in Paragraph 2.2 of this Schedule; |
| **"Replacement Goods"** | any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those services are provided by the Buyer internally and/or by any third party; |
| **"Replacement Services"** | any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those Deliverables are provided by the Buyer internally and/or by any third party; |
| **"Termination Assistance"** | 1. the provision of any configuration information reasonably required to effect the implementation of the Replacement Services excluding the   Core Network;   1. any activity required to facilitate the transition from the live operation of an existing Service to the live operation of a Replacement Service excluding the Core Network; and 2. the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice; |
| **"Termination Assistance**  **Notice"** | has the meaning given to it in Paragraph  5.1 of this Schedule; |
| **"Termination Assistance**  **Period"** | the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule; |
| **"Transferable Assets"** | Exclusive Assets which are capable of legal transfer to the Buyer; |
| **"Transferable Contracts"** | Sub-Contracts, licences for Supplier's  Software, licences for Third Party  Software or other agreements which are |
|  | necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant  Documentation, excluding such contracts  relating to the Core Network; |
| **"Transferring Assets"** | has the meaning given to it in Paragraph  8.2.1 of this Schedule; |
| **"Transferring Contracts"** | has the meaning given to it in Paragraph 8.2.3 of this Schedule. |

#### 2. Supplier must always be prepared for contract exit

2.1 The Supplier shall within 30 days from the Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.

2.2 During the Contract Period, the Supplier shall promptly:

2.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Subcontracts and other relevant agreements required in connection with the Deliverables insofar as they relate to Exclusive Assets and Non Exclusive Assets; and

2.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables (excluding the Core Network) ("**Registers**").

2.3 The Supplier shall:

2.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and

2.3.2 procure that all licences for Third Party Software and all Sub-Contracts in relation to Exclusive and Non-Exclusive Assets shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

2.4 Each Party shall appoint an Exit Manager within three (3) Months of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

#### 3. Assisting re-competition for Deliverables

3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "**Exit Information**").

3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier’s or its Subcontractors’ prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information (excluding the Core Network) which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables (excluding the Core Network); and not be disadvantaged in any procurement process compared to the Supplier.

#### 4. Exit Plan

4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the

Buyer an Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.3 The Exit Plan shall set out, as a minimum:

4.3.1 a detailed description of both the transfer and cessation processes, including a timetable;

4.3.2 how the Deliverables (excluding the Core Network) will transfer to the Replacement Supplier and/or the Buyer;

4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

4.3.4 proposals for the training of key members of the Replacement Supplier’s staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

4.3.7 proposals for the identification and return of all Buyer Assets in the possession of and/or control of the Supplier or any third party;

4.3.8 proposals for the disposal of any redundant Deliverables and materials;

4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

1. every [six (6) months] throughout the Contract Period; and
2. no later than [twenty (20) Working Days] after a request from the Buyer for an up-to-date copy of the Exit Plan;
3. as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than [ten (10) Working Days] after the date of the Termination Assistance Notice;
4. as soon as reasonably possible following, and in any event no later than [twenty (20) Working Days] following, any material change to the Deliverables (including all changes under the Variation Procedure); and

4.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

* 1. Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.
  2. A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

#### 5. Termination Assistance

5.1 The Buyer shall be entitled to require the provision of Termination

Assistance at any time during the Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

5.1.1 the nature of the Termination Assistance required;

5.1.2 the start date and initial period during which it is anticipated that Termination

Assistance will be required, which shall continue no longer than twelve (12) Months after the End Date.; and

5.1.3 whether the Buyer requires any additional services to assist with exit beyond what is required by this Schedule, which may be chargeable by the Supplier.

5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:

5.2.1 no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and

5.2.2 the Buyer shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.

5.3 The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.

5.4 Where the Buyer indicates in a Termination Assistance Notice that it requires any additional services to assist with exit in accordance with paragraph 5.1.3, the Supplier shall provide to the Buyer within ten (10) Working Days of receipt of such Termination Assistance Notice a quotation in the form of an itemised list of costs (in line with any day rates specified in the Contract) for each line of the additional services that the Buyer requires. Within five (5) Working Days of receipt of such quotation the Buyer shall confirm to the Supplier which of those itemised services it requires and the Supplier shall provide those services as part of the Termination Assistance at the Charges provided in the quotation.

5.5 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

#### 6. Termination Assistance Period

6.1 Throughout the Termination Assistance Period the Supplier shall:

6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;

6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI’s) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;

6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.

6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

#### 7. Obligations when the contract is terminated

7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:

7.2.1 vacate any Buyer Premises;

7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

1. such information relating to the Deliverables as remains in the possession or control of the Supplier; and
2. such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

#### 8. Assets, Sub-contracts and Software

8.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

8.1.1 terminate, enter into or vary any Sub-contract insofar as it relates to Exclusive Assets and Non-Exclusive Assets; or

8.1.2 terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables excluding the Core Network; or

8.1.3 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

8.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**"); 8.2.2 which, if any, of:

1. the Exclusive Assets that are not Transferable Assets; and
2. the Non-Exclusive Assets, the Buyer and/or the Replacement Supplier requires the continued use of; and

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

in order for the Buyer and/or its Replacement Supplier to provide the

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

* 1. With effect from the expiry of the Termination Assistance Period, the

Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.

* 1. Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.
  2. Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-

Exclusive Assets, the Supplier shall as soon as reasonably practicable:

* + 1. procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which
    2. procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.
  1. The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.
  2. The Buyer shall:
     1. accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and
     2. once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.
  3. The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.
  4. The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

#### 9. No charges

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

#### 10. Dividing the bills

10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

10.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

10.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

Call-Off Schedule 11 (Installation Works) Call-Off Ref:

Crown Copyright 2018

## Call-Off Schedule 11 (Installation Works)

### 1. When this Schedule should be used

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

### 2. How things must be installed

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

2.1.1. accept the Installation Works, or

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

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

2.3. The Installation Works shall be deemed to be completed when the Supplier receives a notice issued by the Buyer in accordance with Paragraph 2.1.1 Notwithstanding the acceptance of any Installation Works in accordance with Paragraph 2.1.1), the Supplier shall remain solely responsible for ensuring that the Goods and the Installation Works conform to the specification in the Call-Off Order Form (or elsewhere in this Contract). No rights of estoppel or waiver shall arise as a result of the acceptance by the Buyer of the Installation Works.

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

Framework Ref: RM6116

Project Version: v1.0 1

Model Version: v3.0

## Call-Off Schedule 13 (Implementation Plan and Testing) Part A - Implementation

### 1. Definitions

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

|  |  |
| --- | --- |
| **"Delay"** | 1. a delay in the Achievement of a Milestone by its Milestone Date; or 2. a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan; |
| **"Deliverable Item"** | an item or feature in the supply of the  Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan; |
| **"Milestone Payment"** | a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone; |
| **Implementation Period"** | has the meaning given to it in Paragraph 7.1; |

### 2. Agreeing and following the Implementation Plan

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

2.2 The draft Implementation Plan:

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

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

2.3 Following receipt of the draft Implementation Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the Implementation Plan. If the Parties are unable to agree the

contents of the Implementation Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

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

2.5 The Supplier shall monitor its performance against the

Implementation Plan and Milestones (if any) and report to the Buyer on such performance.

### 3. Reviewing and changing the Implementation Plan

3.1 Subject to Paragraph 3.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer’s instructions and ensure that it is updated on a regular basis.

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

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

3.4 Failure by the Supplier to Achieve a Milestone by the relevant Milestone Date, where such failure is caused by or is attributable to the acts and/or omissions of the Supplier shall constitute a material Default and shall entitle the Buyer to terminate the Contract.

### 4. Security requirements before the Start Date

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

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

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

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

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

### 5. What to do if there is a Delay

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

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

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

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

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

### 6. Compensation for a Delay

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

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

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

1. the Buyer is entitled to or does terminate this

Contract pursuant to Clause 10.4 (When CCS or the

Buyer can end this contract); or

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

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

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

Buyer to recover any such damages; and

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

1. **[Implementation Plan** 
   1. The Implementation Period will be a [six (6)] Month period.
   2. During the Implementation Period, the incumbent supplier shall retain full responsibility for all existing services until the Call-Off Start Date or as otherwise formally agreed with the Buyer. The Supplier's full service obligations shall formally be assumed on the Call-Off Start Date as set out in Order Form.
   3. In accordance with the Implementation Plan, the Supplier shall:
      1. work cooperatively and in partnership with the Buyer, incumbent supplier, and other Framework Supplier(s), where applicable, to understand the scope of Services to ensure a mutually beneficial handover of the Services;
      2. work with the incumbent supplier and Buyer to assess the scope of the Services and prepare a plan which demonstrates how they will mobilise the Services;
      3. liaise with the incumbent Supplier to enable the full completion of the Implementation Period activities; and
      4. produce an Implementation Plan, to be agreed by the Buyer, for carrying out the requirements within the Implementation Period including, key Milestones and dependencies.
   4. The Implementation Plan will include detail stating:
      1. how the Supplier will work with the incumbent Supplier and the Buyer Authorised Representative to capture and load up information such as asset data ; and
      2. a communications plan, to be produced and implemented by the Supplier, but to be agreed with the Buyer, including the frequency, responsibility for and nature of communication with the Buyer and end users of the Services.
   5. In addition, the Supplier shall:
      1. appoint a Supplier Authorised Representative who shall be responsible for the management of the Implementation Period, to ensure that the Implementation Period is planned and resourced adequately, and who will act as a point of contact for the Buyer;
      2. mobilise all the Services specified in the Specification within the Call-Off Contract;
      3. produce an Implementation Plan report for each Buyer Premises to encompass programmes that will fulfil all the Buyer's obligations to landlords and other tenants:
         1. the format of reports and programmes shall be in accordance with the Buyer's requirements and particular attention shall be paid to establishing the operating requirements of the occupiers when preparing these programmes which are subject to the Buyer's approval; and
         2. the Parties shall use reasonable endeavours to agree the contents of the report but if the Parties are unable to agree the contents within twenty (20) Working Days of its submission by the Supplier to the Buyer, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
      4. manage and report progress against the Implementation Plan;
      5. construct and maintain a Implementation risk and issue register in conjunction with the Buyer detailing how risks and issues will be effectively communicated to the Buyer in order to mitigate them;
      6. attend progress meetings (frequency of such meetings shall be as set out in the Order Form) in accordance with the Buyer's requirements during the Implementation Period. Implementation meetings shall be chaired by the Buyer and all meeting minutes shall be kept and published by the Supplier; and
      7. ensure that all risks associated with the Implementation Period are minimised to ensure a seamless change of control between incumbent provider and the Supplier.]

### Annex 1: Implementation Plan

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Milest one | | | Deliver able Items | | | Duration | | | Miles tone Date | | | Buyer  Responsibili  ties | | | Milestone Payments | | | | Delay  Payments | | | | |
|  | [ ] |  |  | [ ] |  |  | [ ] |  |  | [ ] |  |  | [ ] |  |  | [ ] |  | |  | [ ] |  | | |
|  |  |  |  |  |  |  | | |  |
|  | | |
| The Milestones will be Achieved in accordance with this Call-Off Schedule 13: (Implementation Plan and Testing) | | | | | | | | | | | | | | | | | | | | | | | |
| For the purposes of Paragraph 6.1.2 the Delay Period Limit shall be | | | | | | | | | | | | | | | | | | **[insert number of** | | | |  | |
|  | **days].** | | | | | | | | | | | | | | | | | | | | | |  |

## Part B - Testing

### 1. Definitions

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

|  |  |
| --- | --- |
| **"Component"** | any constituent parts of the Deliverables; |
| **"Material Test Issue"** | a Test Issue of Severity Level 1 or Severity Level 2; |
| **"Satisfaction**  **Certificate"** | a certificate materially in the form of the document contained in Annex 2 issued by the Buyer when a Deliverable and/or Milestone has satisfied its relevant Test Success Criteria; |
| **"Severity Level"** | the level of severity of a Test Issue, the criteria for which are described in Annex 1; |
| **"Test Issue Management Log"** | a log for the recording of Test Issues as described further in Paragraph 8.1 of this Schedule; |
| **"Test Issue**  **Threshold"** | in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan; |
| **"Test Reports"** | the reports to be produced by the Supplier setting out the results of Tests; |
| **"Test Specification"** | the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in  Paragraph 6.2 of this Schedule; |
| **"Test Strategy"** | a strategy for the conduct of Testing as described further in Paragraph 3.2 of this Schedule; |
| **"Test Success**  **Criteria"** | in relation to a Test, the test success criteria for that Test as referred to in Paragraph 5 of this Schedule; |
| **"Test Witness"** | any person appointed by the Buyer pursuant to Paragraph 9 of this Schedule; and |
| **"Testing Procedures"** | the applicable testing procedures and Test Success Criteria set out in this Schedule. |

### 2. How testing should work

2.1 Part B of this Schedule shall only apply if the Contract was entered into as a result of the Buyer undertaking a Further Competition in accordance with Framework Schedule 7.

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

2.3 The Supplier shall not submit any Deliverable for Testing:

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

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

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

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

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

### 3. Planning for testing

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

3.2 The final Test Strategy shall include:

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

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

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

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

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

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

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

3.2.8 the technical environments required to support the Tests; and

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

### 4. Preparing for Testing

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

4.2 Each Test Plan shall include as a minimum:

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

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

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

### 5. Passing Testing

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

### 6. How Deliverables will be tested

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

6.2 Each Test Specification shall include as a minimum:

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

6.2.2 a plan to make the resources available for Testing;

6.2.3 Test scripts;

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

6.2.5 expected Test results, including:

1. a mechanism to be used to capture and record Test results; and
2. a method to process the Test results to establish their content.

### 7. Performing the tests

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

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

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

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

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

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

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

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

7.6.1 an overview of the Testing conducted;

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

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

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

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

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

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

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

### 8. Discovering Problems

8.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in

Annex 1 and the Test Issue Management Log maintained by the

Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.

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

8.3 The Buyer shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved

Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

### 9. Test witnessing

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

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

9.3 The Test Witnesses:

9.3.1 shall actively review the Test documentation;

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

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

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

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

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

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

### 10. Auditing the quality of the test

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

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

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

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

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

10.6 In the event of an inadequate response to the written report from the

Supplier, the Buyer (acting reasonably) may withhold a Satisfaction Certificate until the issues in the report have been addressed to the reasonable satisfaction of the Buyer.

### 11. Outcome of the testing

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

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

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

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

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

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

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

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

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

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

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

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

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

11.9 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Buyer may at its discretion

(without waiving any rights in relation to the other options) choose to issue a Satisfaction Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:

11.9.1 any Rectification Plan shall be agreed before the issue of a conditional Satisfaction Certificate unless the Buyer agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Buyer within 10 Working

Days of receipt of the Buyer’s report pursuant to Paragraph 10.5); and

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

### 12. Risk

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

12.1.1 operate to transfer any risk that the relevant Deliverable or

Milestone is complete or will meet and/or satisfy the Buyer’s requirements for that Deliverable or Milestone; or

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

## Annex 1: Test Issues – Severity Levels

### 1. Severity 1 Error

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

### 2. Severity 2 Error

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

2.1.1 causes a Component to become unusable;

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

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

### 3. Severity 3 Error

3.1 This is an error which:

3.1.1 causes a Component to become unusable;

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

3.1.3 has an impact on any other Component(s) or any other area of the Deliverables; but for which, as reasonably determined by the Buyer, there is a practicable workaround available;

### 4. Severity 4 Error

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

### 5. Severity 5 Error

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

## Annex 2: Satisfaction Certificate

To: [insert name of Supplier]

From: [insert name of Buyer]

[insert Date dd/mm/yyyy]

Dear Sirs,

### Satisfaction Certificate

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

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

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

[We confirm that all the Deliverables relating to [insert relevant description of Deliverables/agreed Milestones and/or reference number(s) from the Implementation Plan] have been tested successfully in accordance with the Test Plan [or that a conditional

Satisfaction Certificate has been issued in respect of those

Deliverables that have not satisfied the relevant Test Success Criteria].

[OR]

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

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

Yours faithfully

[insert Name] [insert Position]

acting on behalf of [insert name of Buyer]

## Call-Off Schedule 14 (Service Levels)

### 1. Introduction

#### 1.1 The Buyer will specify in the Order Form at

**Further Competition whether Part A or Part B to this Schedule applies or may opt to adopt the Supplier’s offer or Core Terms by omitting this Schedule.**

##### 2. Definitions

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

**“Achieved Service** means the actual level of performance of a Service

**Level”** achieved by the Supplier in relation to a Service

Level Performance Criteria for a Service Period;

means the period during which the Supplier ensures **“Agreed Service**

**Time”** the Services are Available to the Buyer;

**“Available”** a Service shall be “Available” when the Buyer’s end users are able to access and use all its functions at

a level that enables them to carry out their normal duties. Availability shall be construed accordingly;

**“Call-Off Contract** means a consecutive period of twelve (12) Months

**Year”** commencing on the Call-Off Start Date or each

anniversary thereof;

1. Specified by the Buyer where the Buyer selects

**“Critical Service** Part A to this Call-Off Schedule 14; or b) any

**Level Failure”** instance of critical service level failure specified in

Annex 2 to Part B of this Schedule where the Buyer

selects Part B to this Schedule;

|  |  |
| --- | --- |
| **“Downtime”**        **“Imposed Carrier Downtime”**                **“Incident”**      **“Incident**  **Resolution Time”**    **“Planned**  **Downtime”**      **“Provisioning”**      **“Resolution”** | means any period of time within the Agreed Service Time during which a Service is not Available, excluding Planned Downtime    means time during which the Supplier is prevented from supplying the Services due to unavailability of an underlying telecommunications service from a third-party provider on which the Services are dependent. In any instance where the Supplier claims Imposed Carrier Downtime, the Supplier must be able to provide evidence to the satisfaction of the Buyer that the interruption to the Services was in fact due in its entirety to unavailability of the underlying service;    means an unplanned incident or interruption to Services, reduction in the quality of the Services or event which could affect the Services in the future;    means the time taken by the Supplier to  Resolve an Incident, as set out in this Schedule;    means the time agreed in advance in writing  by the Supplier and Buyer within the Agreed Service Time when a Service is not Available;    means the time taken from the placement of  an Order for a Service or part thereof until the Service is Available to the Buyer and Provision shall be construed accordingly; means an action taken by or on behalf of the  Supplier to fully repair the root cause of an Incident or to implement a workaround, such that the Services are returned to being Available. Resolve and Resolved shall be construed accordingly; |
| **"Service Credits"** | a) 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; or |

1. any service credits specified in the Annex to

Part B of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;

|  |  |  |  |
| --- | --- | --- | --- |
| **"Service Credit**  **Cap"** | | 1. in the period from the Call-Off Start Date to the end of the first Call-Off Contract Year [insert cap]; and 2. during the remainder of the Call-Off Contract Period, thirty five percent (35%) of the Charges payable to the Supplier under this Call-Off Contract in the period of twelve (12) Months immediately preceding the Service Period in respect of which Service Credits are accrued;     **unless** otherwise stated in the Order Form during a Further Competition; | |
| **“Service Desk”**        **“Service Failure**  **Threshold”**        **“Service Levels”** | | means the single point of contact set up and operated by the Supplier to log, monitor and escalate Incidents and Incident Resolutions;    means the level of performance of a Service which becomes unacceptable to the Buyer, including as set out in each Service Level Performance Criteria and where the Supplier fails to provide the Services in accordance with this Contract;    means any service levels applicable to the provision of the Services under this Call-Off Contract specified in Call-Off Schedule 14 (Service Levels); | |
| **"Service Level**  **Failure"** | | means a failure to meet the Service Level Threshold in respect of a Service Level Performance Criterion; | |
|  | |  | |
|  | |  | |
| **"Service Level** | | shall be as set out against the relevant Service | |
| **Threshold"**        **“Service Period”**      **“Unavailable”** | Level in Annex 1 to Part A of this Schedule, or Annex 1 of Part B of this Schedule depending upon which option is selected by the Buyer;.    means a recurrent period of one month during the Call-Off Contract Period, unless otherwise specified in the Order Form;    in relation to a Service, means that the Service is not Available; | |

##### 3. What happens if you don’t meet the Service Levels

3.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Threshold for each Service Level.

3.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A or Part B of this Schedule, as appropriate, 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 Threshold.

3.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part C (Performance Monitoring) of this Schedule.

3.4 A Service Credit shall be the Buyer’s exclusive financial remedy for a Service Level Failure except where:

3.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

3.4.2 the Service Level Failure:

1. exceeds the relevant Service Failure Threshold;
2. has arisen due to a Prohibited Act or wilful Default by the Supplier;
3. results in the corruption or loss of any Government Data; and/or
4. results in the Buyer being required to make a compensation payment to one or more third parties; and/or

3.4.3 the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 of the Core Terms (CCS and Buyer Termination Rights).

3.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months’ notice, change the weighting of Service Level Threshold in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:

* + 1. the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;
    2. the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and
    3. there is no change to the Service Credit Cap.

##### 4. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

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

4.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"), provided that the operation of this paragraph 4 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: Short Form 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 Threshold; 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:

1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;

1.2.2 instruct the Supplier to comply with the Rectification Plan Process;

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

1.2.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

### 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 1 to Part A of this Schedule.

## Annex 1 : Short Form Services Levels and Service Credits Table

[**Guidance Note:** The following are included by way of example onlyincluding Service Levels relating to Social Value (Social Value KPIs). Procurementspecific Service Levels should be incorporated. In line with the [Sourcing Playbook,](https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks) it is HMG’s intention to publish the top KPIs for the Government’s most important contracts. Where this publication requirement applies to this Contract, the Buyer must select at least three Service Levels (KPIs) which shall be publishable and must also select the single most important Social Value KPI, which shall also be publishable (four KPIs in total). Buyers can indicate which are publishable in the table below]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Service Levels | | |  | Service Credit for each Service Period |  |
| Service  Level  Performance  Criterion | Key  Indicator | Servic e Level Threshold | Service  Failure  Threshold | Publishable KPI |
| **[**Accurate and timely billing of Buyer] | [Accuracy  /Timelines] | [at least  100% at  all times] | [ ] | [0.5% Service Credit gained for  each percentage under the specified  Service  LevelThreshold] | [Yes] |
| [Access to Buyer support] | [Availability  ] | [at  least 98% during working hours | [ ] | [0.5% Service Credit gained for  each percentage under the specified  Service  LevelThreshold] | [Yes/No] |
| [KPI] | [ ] | [ ] | [ ] | [ ] | [Yes/No] |
| Service Levels | |  |  | Service Credit for each Service Period |  |
| Service  Level  Performance  Criterion | Key  Indicator | Servic e Level Threshold | Service  Failure  Threshold | Publishable KPI |
| [Social Value  KPI 1] | [ ] | [ ] | [ ] | [ ] | [Yes/No] |
| [Social Value  KPI 2] | [ ] | [ ] | [ ] | [ ] | [Yes/No] |
| [Social Value  KPI 3] | [ ] | [ ] | [ ] | [ ] | [Yes/No] |

Critical Service Level Failure

[Buyer Guidance: Buyer to select from below.]

[Insert: Buyers required meaning for Critical Service Level Failure]

OR

[Insert:

1.1 A Critical Service Level Failure will be deemed to have occurred if the performance of the Services falls below the same Service Failure Threshold on three (3) occasions in any six (6) consecutive Service Periods.

|  |  |
| --- | --- |
| 1.2 In the event of a Critical Service Level Failure, the Buyer shall be | |
| entitled to terminate this Call-Off Contract for material Default.] |  |

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

[Example:

Formula: x% (Service Level

Threshold) - x% (actual Service

Level performance)

= x% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice

Worked example: 98% (e.g. Service Level Threshold requirement for accurate and timely billing Service Level) - 75% (e.g. actual performance achieved against this Service Level in a Service Period) payable by the Buyer

= 23% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer]

## PART B: Long Form Service Levels and Service Credits

### 1. General provisions

1.1. The Supplier shall provide support and advice, when required by the Buyer, on matters relating to:

1.1.1. Availability of the Services;

1.1.2. quality of the Services;

1.1.3. provisioning;

1.1.4. essential downtime

1.1.5. Buyer support;

1.1.6. complaints handling; and 1.1.7. accurate and timely invoices.

1.2. The Supplier accepts and acknowledges that failure to meet the Service Level Threshold set out in this Part B of this Call-Off Schedule will result in Service Credits being due to the Buyer.

### 2. Principal points

2.1. The objectives of the Service Levels and Service Credits are to:

2.1.1. incentivise the Supplier to meet the Service Levels and to remedy any failure to meet the Service Levels expeditiously;

2.1.2. ensure that the Services are of a consistently high quality and meet the requirements of the Buyer;

2.1.3. provide a mechanism whereby the Buyer can attain meaningful recognition of inconvenience and/or loss resulting from the Supplier’s failure to deliver the level of service for which it has contracted to deliver; and

2.1.4. provide an incentive to the Supplier to comply with and to expeditiously remedy any failure to comply with the Service Levels.

2.2. The Parties acknowledge that:

2.2.1. The Buyer will, in all cases, prefer to receive the Services within the

Service Levels in preference to receiving the Service Credits; and

2.2.2. the Supplier shall, in all cases, seek to deliver the Services within the Service Levels in preference to accepting a liability for Service Credits.

### 3. Service Levels

3.1. The Supplier shall monitor its performance under this Call-Off Contract by reference to the relevant Service Level Performance Criteria for achieving the Service Levels and shall send the Buyer a Performance Monitoring Report detailing the level of service which was achieved in accordance with the provisions of Part C (Performance Monitoring) of this Call-Off Schedule.

3.2. The Supplier shall, at all times, provide the Services in such a manner that the Service Level Thresholds are achieved.

3.3. If the level of performance of the Supplier of any element of the provision by it of the Services during the Call-Off Contract period:

3.3.1. is likely to or fails to meet any Service Level Threshold; or

3.3.2. is likely to cause or causes a Critical Service Level Failure to occur, the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without prejudice to any other of its rights howsoever arising may:

1. Require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring; and

1. If the action taken under paragraph 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; and above has not already prevented or remedied the Service Level Failure or Critical Service Level Failure, the Buyer shall be entitled to instruct the Supplier to comply with the Rectification Plan Process; or

1. If a Service Level Failure has occurred, deduct from the Call-Off

Contract Charges the applicable Service Credits payable by the Supplier to the Buyer in accordance with the calculation formula set out in Annex 1 of this Part B of this Call-Off Schedule; or

1. If a Critical Service Level Failure has occurred, exercise its right to compensation for such non-availability of Services via this Call-Off Contract.

* 1. Approval and implementation by the Buyer of any Rectification Plan shall not relieve the Supplier of any continuing responsibility to achieve the Service Levels, or remedy any failure to do so, and no estoppels or waiver shall arise from any such Approval and/or implementation by the Buyer.

* 1. The Buyer may enhance or otherwise modify the Service Levels required during a Further Competition Procedure.

* 1. The Services are subject to the following four Service Level Performance Criteria as set out in paragraph 6 of this Part B of Call-Off Schedule 14:

* + 1. Availability;

* + 1. Incident Resolution;

* + 1. Quality; and

* + 1. Provisioning.

### 4. Agreed Service Time

4.1. The Services will be made Available by the Supplier to the Buyer during the Agreed Service Time.

4.2. The Agreed Service Time applied to the Services will be determined by the Service Maintenance Level selected by the Buyer on the Order Form.

4.3. The Service Maintenance Levels and associated Agreed Service Times is set out in the following table:

|  |  |
| --- | --- |
| Service  Maintenance Level | Agreed Service Time |
| Level 1 | Monday – Friday (excluding Bank Holidays) 08:00-18:00 |
| Level 2 | Monday – Saturday (excluding Bank Holidays) 08:00-18:00 |
| Level 3 | Monday – Sunday (including Bank Holidays) 07:00-21:00 |
| Level 4 | Monday – Sunday (including Bank Holidays); 00:00-23:59  (24 hours per day, 7 days per week) |

### 5. Incidents

5.1. If the Services become Unavailable, the Buyer must report the Unavailability as an Incident to the Service Desk.

5.2. Incidents must be classified to one of the following four severity levels:

|  |  |
| --- | --- |
| Severity Level | Description of impact of Incident |
| Severity 1 | The Services are Unavailable across the entire Buyer’s estate |
| Severity 2 | The Services are Unavailable at one of the Buyer’s sites |
| Severity 3 | The Services are Unavailable to an individual user |
| Severity 4 | All other Incidents, including any Incidents raised initially at a higher Severity Level that were subsequently deemed to be attributable to the Buyer or in any other way not attributable to the Supplier. |

5.2.1. The Supplier shall manage the Incident to resolution in accordance with this Call-Off Schedule, whilst keeping the Buyer appropriately informed of progress.

### 6. Service Level Performance Criteria

#### 6.1. Availability

6.1.1. The Supplier shall ensure that the Services are Available during the Agreed Service Time.

6.1.2. Achieved Availability is calculated as a percentage of the total time in a Service Period that the Services should have otherwise been Available to the Buyer using the following formula:

### (MP – SD) x 100

Achieved Availability % =

MP Where:

MP means total time within the Agreed Service Time (excluding Planned

Downtime, Imposed Carrier Downtime and any Unavailability attributable to Severity 3 or Severity 4 Incidents) within the relevant Service Period; and

SD means total service downtime within the Agreed Service Time within the relevant Service Period during which a Service and/or part thereof is Unavailable (excluding Planned Downtime, Imposed Carrier Downtime and any Unavailability attributable to Severity 3 or Severity 4 Incidents) within the relevant Service Period.

#### 6.2. Incident Resolution

6.2.1. The Supplier shall ensure that Incidents are resolved within the Maximum Incident Resolution Time.

6.2.2. Maximum Incident Resolution Times are determined by the Severity Levels and Service Maintenance Levels as set out in the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| Service  Maintenance Level | Severity 1; and  Severity 2 | Severity 3 | Severity 4  (Indicative Only) |
| Level 1 | End of next Working Day | 5 Working  Days | 1 Month |
| Level 2 | End of next Working Day | 5 Working  Days | 1 Month |
| Level 3 | Incident reported by 13:00, resolved same day; reported after 13:00, resolved by 13:00 next Working Day | End of next Working Day | 15 Working Days |
| Level 4 | 6 hours | End of next Working Day | 10 Working Days |

6.2.3. Each Incident will either be Resolved within the Maximum Incident

Resolution Time, or it will not; and will be reported as such by the Supplier. The time taken to resolve the Incident is not material to this Service Level Performance Criteria.

6.2.4. Achieved Incident Resolution is calculated as a percentage of the total number of Incidents in a Service Period that should have been resolved within the Maximum Incident Resolution Time using the following formula:

Achieved Incident (TI-FI) x 100

=

Resolution % TI

Where:

TI means the total number of Incidents raised by the Buyer during the Service Period (excluding Severity 4 Incidents); and

FI means the total number of Incidents raised by the Buyer during the Service Period that were not resolved within the Maximum Incident Resolution Time (excluding Severity 4 Incidents).

6.2.5. Where an Incident is reported outside the Agreed Service Time, the Incident will be treated as if it has been reported at the beginning of the next Working Day.

6.2.6. The Incident will only be deemed to be Resolved once the Services are Available. However, the Supplier shall not formally close any Incident until the Buyer has confirmed that the Services are Available.

#### 6.3. Quality

6.3.1. The Supplier shall ensure that the Services are delivered of a sufficient quality to meet the provisions of this Call-Off Schedule.

6.3.2. Measurement of answer and response times of the Service Desk will be based on the time taken for the Supplier to respond to the Buyer’s call or email. Calls and emails receiving an automated response or calls placed into a queuing system shall be deemed not to have been answered.

#### 6.4. Provisioning

6.4.1. The Services will be provisioned at the outset in accordance with any Implementation Plan and any failure to meet Milestones will be dealt with in accordance with the terms of this Call-Off Contract.

6.4.2. Any delivery of Services or part thereof subsequent to the successful conclusion of the Implementation Plan will be subject to the Service Levels identified in the Variation to this Contract that incorporates those changes; or failing any other agreed Service Level, in accordance with the Supplier’s standard provisioning Service Levels.

#### 7. Service Credits

7.1. This section sets out the basic agreed formula used to calculate a Service Credit payable to the Buyer as a result of a Service Level Failure in a given Service Period.

7.2. Service Credit payments are subject to the Service Credit Cap.

7.3. Annex 1 to this Part B of this Call-Off Schedule details the Service Credits available for each Service Level Performance Criterion in the event that the applicable Service Level Threshold is not met by the Supplier.

7.4. The Buyer shall use the Performance Monitoring Reports supplied by the Supplier under Part C (Performance Monitoring) of this Call-Off Schedule to verify the calculation and accuracy of any Service Credits applicable to each Service Period.

7.5. Service Credits are a reduction of the amounts payable in respect of the Services 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 Annex 1 of Part B of this Call-Off Schedule.

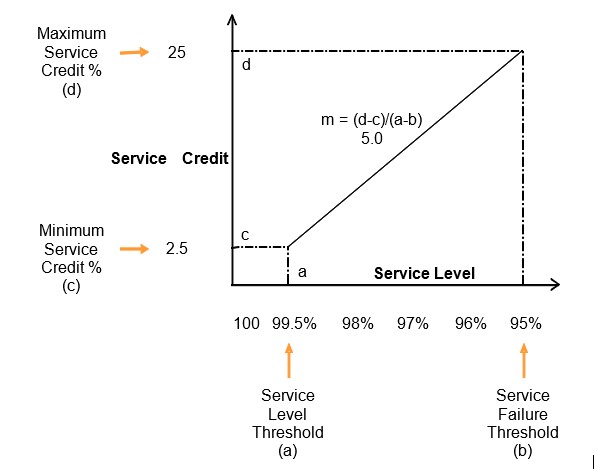
7.6. The amount of Service Credit is determined by the tables in Annex 1 of this Part B of Call-Off Schedule 14, using the calculated Achieved Service Level Performance Criteria (e.g. Achieved Availability), the Service Level Threshold and the Service Failure Threshold and is calculated by using the straight line formula below:

**Service Credit % = (m\*(a-x) + c), where** *a* is the Service Level Threshold (%) below which Service Credits become payable; *b* is the Service Failure Threshold (%); *x* is the Achieved Service Level Performance Criteria (%) for a Service Period; *c* is the minimum Service Credit (%) payable if the Achieved Service Level falls below the Service Level Threshold;

*d* is the maximum Service Credit (%) payable if the Achieved Service Level Reaches the Service Failure Threshold;

*m* is a coefficient defined for the services, which is calculated from the Formula m = (d-c)/(a-b), that is the slope of the straight line;

7.7. Consequently, the Service Credit regime is shown diagrammatically as follows:



7.8. The Service Credit (£) is subsequently derived as follows: **Service Credit (£) = contract charges x Service Credit (%)**

7.9. An example Service Credit calculation for the Availability of a service, (offered herein for illustrative purposes only), is as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Criteria | Coefficient (m) | Service Level Threshold % (a) | Service  Failure  Threshold %  (b) | Minimum  Service  Credit %  (c) | Maximum  Service  Credit % (d) |
| Availability | 5.0 | 99.5% | 95.00 % | 2.5 % | 25% |

7.9.1. The Achieved Availability of a service was recorded as 97% for a Service Period. For this service, the Service Level Threshold is 99.5% and the Service Failure Threshold is 95%. The contract charges for the service for the Service Period are £3,000. Previous performance had exceeded the Service Level Threshold for Availability.

7.9.2. In this illustration example:

Service Credit % = 5.0 x (99.5-97.0) + 2.5 = 15%;

therefore the Service Credit calculation is:

Service Credit (£) = £3,000 x 15% = £450.

7.10. An example Service Credit calculation for Incident Resolution is as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Criteria | Coefficient (m) | Service  Level  Threshold %  (a) | Service  Failure  Threshold %  (b) | Minimum  Service  Credit % (c) | Maximum  Service  Credit % (d) |
| Incident  Resolution | 0.25 | 95.0% | 85.00% | 2.5% | 5% |

7.10.1. The Service Level Threshold is 95% of all incidents to be resolved within a specified time with the Service Failure Threshold being 85%. Assume that the Buyer has 80 Incidents within a Service Period, 10 of which were not resolved within the specified time. Therefore, the Achieved Incident Resolution is 87.5% for the Service Period. The contract charges for all the services that the Buyer is consuming are £50,000 per Service Period. Previous performance had exceeded the Service Level Threshold for Incident Resolution Times.

7.10.2. In this illustration example:

Service Credit % = 0.25 x (95-87.5) + 2.5 = 4.375%

Consequently, the illustrated Service Credit calculation is:

Service Credit (£) = £50,000 x 4.375% = £2,187.50.

## PART B Annex 1: Long Form Services Levels and Service Credits Table

### 1. Availability

#### 1.1. Services (excluding the Service Desk)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Service  Maintenance  Level | Coefficient (m) | Service  Level  Threshold  % (a) | Service  Failure  Threshold  % (b) | Minimum  Service  Credit %  (c) | Maximum  Service  Credit %  (d) |
| 1 | N/A | N/A | N/A | N/A | N/A |
| 2 | 1.3 | 95% | 80% | 5% | 25% |
| 3 | 2.86 | 97% | 90% | 5% | 25% |
| 4 | 5 | 99% | 95% | 5% | 25% |

#### 1.2. Service Desk

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Service  Maintenance  Level | Coefficient (m) | Service  Level  Threshold  % (a) | Service  Failure  Threshold  % (b) | Minimum  Service  Credit %  (c) | Maximum  Service  Credit % (d) |
| All | 5 | 99% | 95% | 5% | 25% |

### 2. Incident Resolution

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Number of Incidents per Service  Period | Coefficient (m) | Service  Level  Threshold  %(a) | Service  Failure  Threshold %  (b) | Minimum  Service  Credit % (c) | Maximum  Service  Credit % (d) |
| 39 or fewer | Not applicable | No more than 2 Incidents are Resolved in excess of the max Incident  Resolution  Times | 5 or more  Incidents are Resolved in excess of the max Incident  Resolution  Times | 2.5%  (payable when 3 Incidents breach the  Service  Level Threshold in any Service  Period) | 5%  (payable when 4+ Incidents breach the  Service  Level Threshold in any Service  Period) |
| 40 and more | 0.25 | 95% | 85% | 2.5% | 5% |

### 3. Quality

3.1. Service Desk:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Criteria | Coefficient | Service  Level  Threshold | Service  Failure  Threshold | Minimum  Service  Credit | Maximum  Service  Credit |
| Calls  Answered within 60 seconds | 0.25 | 90% | 80% | 2.5% | 5% |
| Email  Responded to within one (1)  Working Day | 0.083 | 90% | 60% | 2.5% | 5% |
| Abandoned  Calls | 0.25 | 95% | 85% | 2.5% | 5% |

#### 3.2. Data Service

3.2.1. Where the Buyer has procured Services that include data services, the following provisions will apply:

1. The Services will only be deemed to have been Delivered once the

Buyer has tested and accepted the quality of the data service;

1. Subsequent to Services commencement, where the Buyer believes the quality of the data service is not acceptable:

(i) an Incident will be raised with the Service Desk (ii) the Supplier shall investigate the Incident; (iii) Subsequent to the investigation, if:

* 1. a fault is found, the Incident is Resolved as any other

Incident;

* 1. a fault is not found and the Buyer still believes the quality of the data service is unacceptable, the Supplier shall evidence to the Buyer that the data service complies with relevant Standards.

(iv) In the event that a fault is not found and the Supplier cannot evidence to the satisfaction of the Buyer that the data service complies with relevant Standards, the Service will be deemed Unavailable from the time that the Incident was first raised with the Service Desk and the Incident Resolution Time will be accordingly measured from that time.

#### 3.3. Voice Service

3.3.1. Where the Buyer has procured Services that include voice services, the following provisions will apply:

1. The Services will only be deemed to have been Delivered once the

Buyer has tested and accepted the quality of the voice service;

1. Subsequent to Services commencement, where the Buyer believes the quality of the voice service is not acceptable:

(i) an Incident will be raised with the Service Desk; (ii) the Supplier shall investigate the Incident; (iii) Subsequent to the investigation, if:

* 1. a fault is found, the Incident is Resolved as any other Incident;
  2. a fault is not found and the Buyer still believes the quality of the voice service is unacceptable, the Supplier shall evidence to the Buyer that the voice service complies with relevant Standards.

(iv) In the event that a fault is not found and the Supplier cannot evidence to the satisfaction of the Buyer that the voice service complies with relevant Standards, the Service will be deemed Unavailable from the time that the Incident was first raised with the Service Desk and the Incident Resolution Time will be accordingly measured from that time.

## PART B Annex 2: Critical Service Level Failure

### 1. CRITICAL SERVICE LEVEL FAILURE

1.1. A Critical Service Level Failure will be deemed to have occurred if the performance of the Services falls below the same Service Failure Threshold on three (3) occasions in any six (6) consecutive Service Periods.

1.2. In the event of a Critical Service Level Failure, the Buyer shall be entitled to terminate this Call-Off Contract for material Default.

## Part C: Performance Monitoring

### 1. Performance Monitoring and Performance Review

1.1. Part C to this Call-Off Schedule provides the methodology for monitoring the provision of the Services:

1.1.1. to ensure that the Supplier is complying with the Service Levels; and

1.1.2. for identifying any failures to achieve Service Levels in the performance of the Supplier and/or provision of the Services (may also be referred to as a "Performance Monitoring System").

1.2. 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.

1.3. The Supplier shall report all failures to achieve Service Levels and any Critical Service Level Failure to the Buyer in accordance with the processes agreed in Paragraph 1.2 of Part C of this Call-Off Schedule above.

1.4. The Supplier shall provide the Buyer with performance monitoring reports ("Performance Monitoring Reports") in accordance with the process and timescales agreed pursuant to paragraph 1.2 of Part C of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

1.4.1. for each Service Level, the actual performance achieved over the

Service Level for the relevant Service Period;

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

1.4.3. details of any Critical Service Level Failures;

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

1.4.5. 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

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

1.5. The Parties shall attend meetings to discuss Performance Monitoring Reports

**("Performance Review Meetings")** on a Monthly basis. The Performance

Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

1.5.1. 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;

1.5.2. be attended by the Supplier's Representative and the Buyer’s Representative; and

1.5.3. 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.

1.6. 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.

1.7. The Supplier shall provide to the Buyer such documentation as the Buyer

may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

### 2. Satisfaction Surveys

2.1. 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.

## PART C ANNEX 1: ADDITIONAL PERFORMANCE MONITORING REQUIREMENTS

[Guidance Note: Where the Buyer has stipulated on the Order Form during a Further Competition Procedure, insert details of any additional performance monitoring requirements here.]

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

### 1. DEFINITIONS

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

|  |  |
| --- | --- |
| **"Operational Board"** | the board established in accordance with paragraph  4.1 of this Schedule; |
| **"Project Manager"** | the manager appointed in accordance with paragraph 2.1 of this Schedule; |

### 2. PROJECT MANAGEMENT

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

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

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

### 3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager shall be:

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

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

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

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

3.2 The Buyer may provide revised instructions to the Supplier's Contract

Manager in regards to the Contract and it will be the Supplier's Contract

Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier's Contract Manager's by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

### 4. ROLE OF THE OPERATIONAL BOARD

4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.

4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.

4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.

4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member’s attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.

4.5 The purpose of the Operational Board meetings will be to review the Supplier’s performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

### 5. Contract Risk Management

5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.

5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

5.2.1 the identification and management of risks; 5.2.2 the identification and management of issues; and

5.2.3 monitoring and controlling project plans.

5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

5.4 The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer and the Supplier have identified.

## Annex: Contract Boards

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

[**Guidance note**: Details of additional boards to be inserted.

**Off Schedule 18 (Background Checks)** Off Ref:

Crown Copyright 2018

## Call-Off Schedule 18 (Background Checks)

### 1. When you should use this Schedule

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

### 2. Definitions

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

### 3. Relevant Convictions

3.1.1 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.

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

1. 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 SubContractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

Framework Ref: RM6116

Project Version: v1.0 1

Model Version: v3.0

**Off Schedule 18 (Background Checks)** Off Ref:

Crown Copyright 2018

## Annex 1 – Relevant Convictions

**[Insert** Relevant Convictions here]

Framework Ref: RM6116

Project Version: v1.0 2

Model Version: v3.0



**Certificate Of Completion**

Envelope Id: 244C3E528C7D40ACBFA539901B805085 Status: Completed

Subject: Complete with Docusign: RM6116-Framework-Schedule-6-Order-Form-Template - CCET\_final version, C...

Source Envelope:

|  |  |  |
| --- | --- | --- |
| Document Pages: 244 Signatures: 1 | | Envelope Originator: |
| Certificate Pages: 5 Initials: 0 | |  |
| AutoNav: Enabled  EnvelopeId Stamping: Enabled  Time Zone: (UTC) Dublin, Edinburgh, Lisbon, London | |  |
| **Record Tracking** |  |  | |
| Status: Original  19-11-24 | 14:13 | Holder: | Location: DocuSign | |
| **Signer Events** | **Signature** | **Timestamp** | |
| Director  Security Level: Email, Account Authentication (None)  **Electronic Record and Signature Disclosure:** | Signature Adoption: Pre-selected Style  Using IP Address:  Signed using mobile | Sent: 19-11-24 | 14:19  Viewed: 19-11-24 | 19:54  Signed: 19-11-24 | 19:56 | |
| **In Person Signer Events** | **Signature** | **Timestamp** | |
|  |  |  | |
| **Editor Delivery Events** | **Status** | **Timestamp** | |
|  |  |  | |
| **Agent Delivery Events** | **Status** | **Timestamp** | |
|  |  |  | |
| **Intermediary Delivery Events** | **Status** | **Timestamp** | |
|  |  |  | |
| **Certified Delivery Events** | **Status** | **Timestamp** | |
|  |  |  | |
| **Carbon Copy Events** | **Status** | **Timestamp** | |
| UKISA  Security Level: Email, Account Authentication (None)  **Electronic Record and Signature Disclosure:**  Not Offered via DocuSign |  | Sent: 19-11-24 | 14:19  Viewed: 20-11-24 | 08:36 | |
| **Witness Events** | **Signature** | **Timestamp** | |
|  |  |  | |
| **Notary Events** | **Signature** | **Timestamp** | |
|  |  |  | |
| **Envelope Summary Events** | **Status** | **Timestamps** | |
| Envelope Sent | Hashed/Encrypted | 19-11-24 | 14:19 | |
| Certified Delivered | Security Checked | 19-11-24 | 19:54 | |
| Signing Complete | Security Checked | 19-11-24 | 19:56 | |
| Completed | Security Checked | 19-11-24 | 19:56 | |
| **Payment Events** | **Status** | **Timestamps** | |

|  |
| --- |
| **Electronic Record and Signature Disclosure** |

Electronic Record and Signature Disclosure created on: 12-10-22 | 18:01

Parties agreed to: Stuart Aldridge

**ELECTRONIC RECORD AND SIGNATURE DISCLOSURE**

From time to time, Mitel - DSfSF (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to ‘I agree to use electronic records and signatures’ before clicking ‘CONTINUE’ within the DocuSign system.

**Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

**Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

**Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

**All notices and disclosures will be sent to you electronically**

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

**How to contact Mitel - DSfSF:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows: To contact us by email send messages to:

**To advise Mitel - DSfSF of your new email address**

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at cmg@mitel.com and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

**To request paper copies from Mitel - DSfSF**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to cmg@mitel.com and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

**To withdraw your consent with Mitel - DSfSF**

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

1. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
2. send us an email to and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

**Required hardware and software**

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: [https://support.docusign.com/guides/signer-guidesigning-system-requirements.](https://support.docusign.com/guides/signer-guide-signing-system-requirements)

**Acknowledging your access and consent to receive and sign documents electronically**

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to ‘I agree to use electronic records and signatures’ before clicking ‘CONTINUE’ within the DocuSign system.

By selecting the check-box next to ‘I agree to use electronic records and signatures’, you confirm that:

* You can access and read this Electronic Record and Signature Disclosure; and
* You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
* Until or unless you notify Mitel - DSfSF as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Mitel - DSfSF during the course of your relationship with Mitel - DSfSF.