Direct Award Order Form Template

Direct award Order Form Template

CALL-OFF REFERENCE:

THE BUYER: Cabinet Office

BUYER ADDRESS:

SUPPLIER REFERENCE NA

THE SUPPLIER: Colt Technology Services

SUPPLIER ADDRESS:

REGISTRATION NUMBER: 2452736

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 01 August 2023.
It's issued under the Framework Contract with the reference number RM3808 for the provision of Network Services.

CALL-OFF LOT(S):
4

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) RM3808
3. The following Schedules in equal order of precedence:

Joint Schedules for framework reference number RM3808

- Joint Schedule 2 (Variation Form)
- Joint Schedule 3 (Insurance Requirements)
- Joint Schedule 7 (Financial Difficulties)

- Call-Off Schedules for **N/A** Call-Off reference number]
  - Call-Off Schedule 5 (Pricing Details)
  - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  - Call-Off Schedule 9 (Security)
  - Call-Off Schedule 14 (Service Levels)

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

CALL-OFF SPECIAL TERMS
N/A

CALL-OFF START DATE	**01 August 2023**
CALL-OFF EXPIRY DATE	**31 July 2025**
CALL-OFF INITIAL PERIOD	**2 Years**

CALL-OFF OPTIONAL EXTENSION PERIOD 2 Years (1 + 1)

MINIMUM PERIOD OF NOTICE FOR WITHOUT REASON TERMINATION

90 Days

CALL-OFF DELIVERABLES

The Supplier will provide the Buyer with:
Service = COLT Dark Fibre, Metro, Single Pair, A: Fibre, G.652, SC/PC, B: Fibre, G.652, SC/PC

Location A =
Location B =

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:
£12,655

CALL-OFF CHARGES

Pricing = Install: £835; Monthly: £985.

Year 1= £12,655
Year 2= £11,820

Optional extensions:
Year 3= £11,820
Year 4 = £11,820

Total contract value: **£48,115**

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4 and 5 in Framework Schedule 3 (Framework Prices).

The Charges will not be impacted by any change to the Framework Prices.

REIMBURSABLE EXPENSES
Not recoverable

PAYMENT METHOD
BACS

BUYER'S INVOICE ADDRESS:
Cabinet Office

BUYER'S AUTHORISED REPRESENTATIVE
Name:
Role:
Email Address:
Address:

BUYER'S ENVIRONMENTAL POLICY
N/A

ADDITIONAL INSURANCES
N/A

GUARANTEE
N/A

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)]

STAFF TRANSFER
N/A

QUALITY PLAN
N/A

MAINTENANCE OF ICT ENVIRONMENT
N/A

BUSINESS CONTINUITY AND DISASTER RECOVERY
In accordance with Call-Off Schedule 8 (Business Continuity and Disaster Recovery) Part A, the Supplier's BCDR Plan at Annex 1 will apply.

SECURITY REQUIREMENTS
In accordance with Call-Off Schedule 9, Part A (Short Form Security)

BUYER'S SECURITY POLICY
N/A

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)
N/A

CLUSTERING
N/A

SERVICE LEVELS AND SERVICE CREDITS
Service Levels applicable to this Call-Off Contract are detailed in Call-Off Schedule

14.

The Service Period is One (1) Month.

SUPPLIER'S AUTHORISED REPRESENTATIVE

SUPPLIER'S CONTRACT MANAGER

KEY STAFF
N/A

KEY SUBCONTRACTOR(S)
N/A

COMMERCIALLY SENSITIVE INFORMATION
N/A

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:		Signature:	
Name:		Name:	
Role:		Role:	
Date:		Date:	

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)

Contact Details		
This variation is between:		
Contract name:		
Contract reference number:		
Details of Proposed Variation		
Variation initiated by:		
Variation number:		
Date variation is raised:		
Proposed variation		
Reason for the variation:		
An Impact Assessment shall be provided within:		
Impact of Variation		
Likely impact of the proposed variation:		
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows:	
Financial variation:	Original Contract Value:	
	Additional cost due to variation:	
	New Contract value:	

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 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 Buyer

Signature	
Date	
Name (in Capitals)	
Address	

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

Signature	
Date	
Name (in Capitals)	
Address	

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need to have

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 l 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 non-renewal 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 The Supplier shall ensure that any Insurances which are stated to have a minimum l 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. 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.

1. ANNEX: Required Insurances

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

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

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

   1.3. employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

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

2.

Joint Schedule 7 (Financial Difficulties)

1. Definitions

1.1 In this Schedule, 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 Annex 2 and

"Financial Distress Event" the occurrence or one or more of the following events:

a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold;

b) 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;

c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party;

d) Monitored Company committing a material breach of covenant to its lenders;

e) 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:

i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract;

ii) non-payment by the Monitored Company of any financial indebtedness;

iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or

iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company

in each case which CCS 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"	the Supplier, any [Framework Guarantor or Call-Off Guarantor or any Key Subcontractor]
"Rating Agencies"	the rating agencies listed in Annex 1.

2. When this Schedule applies

2.1 The Parties shall comply with the provisions of this Schedule 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 Schedule shall apply to all Call-Off Contracts unless:

2.2.1 where the Buyer has conducted a direct award from the Catalogue the Supplier has indicated in the relevant Service Offer that Joint Schedule 7 shall not apply; or

2.2.2 where specified by a Buyer that has undertaken a Further Competition that this Schedule shall not apply.

2.3 The terms of this Schedule shall survive:

2.3.1 under the Framework Contract until the later of (a) the termination or Expiry Date of the Framework Contract; or (b) the latest date of termination or Expiry Date of any Call-Off Contract entered into under the Framework Contract (which might be after the date of termination or Expiry Date of the Framework Contract); and

2.3.2 under the Call-Off Contract until the termination or Expiry Date of the Call-Off Contract.

3. What happens when your credit rating changes

3.1 The Supplier warrants and represents to CCS 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 Annex 2.

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

3.3 If there is any downgrade credit rating issued by any Rating Agency for either the Monitored Company the Supplier shall ensure that the Monitored Company's auditors thereafter provide CCS within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by CCS (such requests not to exceed 4 in any Contract Year) with written calculations of the quick ratio for the Monitored Company

be as at the end of each Contract Year or such other date as may be requested by CCS. For these purposes the "quick ratio" on any date means:

$$\frac{A+B+C}{D}$$

where:

A is the value at the relevant date of all cash in hand and at the bank of the Monitored Company;

B is the value of all marketable securities held by **the Monitored Company** determined using closing prices on the Working Day preceding the relevant date;

C is the value at the relevant date of all account receivables of the Monitored Company; and

D is the value at the relevant date of the current liabilities of the Monitored Company.

3.4 The Supplier shall:

3.4.1 regularly monitor the credit ratings of each Monitored Company with the Rating Agencies; and

3.4.2 promptly notify (or shall procure that its auditors promptly notify) CCS 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.

3.5 For the purposes of determining whether a Financial Distress Event the credit rating of the Monitored Company (as the case may be) 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

4.1 In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if CCS 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 CCS shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

4.2 In the event that a Financial Distress Event arises due to a Key Subcontractor notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute then, CCS 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 CCS's reasonable satisfaction that there is a valid reason for late or non-payment.

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

4.3.1 at the request of CCS meet CCS 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

4.3.2 where CCS 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:

(a) submit to CCS 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

(b) provide such financial information relating to the Monitored Company as CCS may reasonably require.

4.4 If CCS 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 CCS 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 CCS or referred to the Dispute Resolution Procedure.

4.5 If CCS 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.

4.6 Following Approval of the Financial Distress Service Continuity Plan by CCS, the Supplier shall:

4.6.1 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;

4.6.2 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

4.6.3 comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).

4.7 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 CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.

4.8 CCS shall be able to share any information it receives from the Supplier in accordance with this Paragraph with any Buyer who has entered into a Call-Off Contract with the Supplier.

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

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

5.1.1 the Supplier fails to notify CCS of a Financial Distress Event in accordance with Paragraph 3.4; and/or

5.1.2 CCS 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

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

6. What happens If your credit rating is still good

6.1 Without prejudice to the Supplier's obligations and CCS' rights and remedies under Paragraph 4, 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:

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

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

1. ANNEX 1: Rating Agencies

Rating Agency 1: Dun & Bradstreet

Rating Agency 2: Experian

2. ANNEX 2: Credit Ratings & Credit Rating Thresholds

Part 1: Current Rating

Entity	Credit rating (long term)	Credit Rating Threshold
Supplier	[to be populated with the Supplier's D&B and Experian ratings at the point of award]]	D&B Risk Indicator 2 – Lower than average risk Experian - Fair
[Framework Guarantor]	[to be populated with the Framework Guarantor's D&B and Experian ratings as at the point of award]	[D&B Risk Indicator 2 – Lower than average risk Experian – Good]
[Call-Off Guarantor]	[to be populated with the Call-Off Guarantor's D&B and Experian ratings as at the point of award]	[to be populated by the Relevant Buyer]
[Key Subcontractor – Call-Off]	[to be populated with the Key Subcontractor's D&B and Experian ratings at the point of Call-Off award]	[to be populated by the Buyer invoking the provision as part of a Further Competition]

RM3808 Call-Off Schedule 5 (Pricing Details)

Dark Fibre Circuit Quote.pdf

RM3808 Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

1. PART A: Supplier BCDR Plan

1. BCDR Plan

1.1. Where the Buyer has not specified a bespoke BCDR Plan in accordance with Part B as part of a Further Competition Procedure, the Supplier's BCDR Plan at Annex 1 to this Part A will apply.

1.2. 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.

1.3. The Supplier's BCDR Plan shall as a minimum detail the processes and arrangements that the Supplier shall follow to:

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

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

2. PART A: ANNEX 1 Supplier BCDR Plan

[**Guidance Note:** Append the Supplier's submitted BCDR Plan from the Tender.]

3. PART B: Bespoke BCDR Plan

1. Introduction

1.1. The following paragraphs 2 to 10 shall apply where the Buyer has as part of a Further Competition required that the Supplier provides a bespoke BCDR Plan.

2. Definitions

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

"BCDR Plan"	has the meaning given to it in Paragraph 3.2 of this Schedule;
"Business Continuity Plan"	has the meaning given to it in Paragraph Section 2 which shall relate to business continuity (the "Business Continuity Plan"); and of this Schedule;
"Disaster Recovery Plan"	has the meaning given to it in Paragraph Section 3 which shall relate to disaster recovery (the "Disaster Recovery Plan") 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;
"Disaster Recovery Deliverables"	the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	has the meaning given to it in Paragraph Error: Reference source not found of this Schedule; and
"Supplier's Proposals"	has the meaning given to it in Paragraph Error: Reference source not found of this Schedule;

3. BCDR Plan

3.1. 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

3.2. At least 10 Working Days prior to the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan, which shall detail the processes and arrangements that the Supplier shall follow to:

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

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

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

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

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

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

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

4. General Principles of the BCDR Plan (Section 1)

4.1. Section 1 of the BCDR Plan shall:

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

4.1.2. 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;

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

4.1.4. detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;

4.1.5. 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;

4.1.6. contain a risk analysis, including:

(a) failure or disruption scenarios and assessments of likely frequency of occurrence;

(b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;

(c) identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and

(d) a business impact analysis of different anticipated failures or disruptions;

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

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

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

4.1.10. 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;

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

4.1.12. provide for the provision of technical assistance to key contacts at the Buyer as reasonably required by the Buyer to inform decisions in support of the Buyer's business continuity plans.

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

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

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

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

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

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

4.4. The Supplier shall not be entitled to any relief from its obligations under the 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.

5. Business Continuity (Section 2)

5.1. 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:

5.1.1. 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

5.1.2. 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.

5.2. The Business Continuity Plan shall:

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

5.2.2. 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;

5.2.3. specify any applicable Service Levels with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and

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

6. Disaster Recovery (Section 3)

6.1. 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.

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

6.2.1. loss of access to the Buyer Premises;

6.2.2. loss of utilities to the Buyer Premises;

6.2.3. loss of the Supplier's helpdesk;

6.2.4. loss of a Subcontractor;

6.2.5. emergency notification and escalation process;

6.2.6. contact lists;

6.2.7. staff training and awareness;

6.2.8. BCDR Plan testing;

6.2.9. post implementation review process;

6.2.10. any applicable Service Levels with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;

6.2.11. 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;

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

6.2.13. testing and management arrangements.

7. Review and changing the BCDR Plan

7.1. The Supplier shall review the BCDR Plan:

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

7.1.2. within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 9; and

7.1.3. where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 7.1.1 and 7.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.

7.2. Each review of the BCDR Plan pursuant to Paragraph 7.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.

7.3. 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.

7.4. 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.

7.5. 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.

2.

3.

8. Testing the BCDR Plan

8.1. The Supplier shall test the BCDR Plan:

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

8.1.2. in the event of any major reconfiguration of the Deliverables;

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

8.2. 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.

8.3. 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.

8.4. 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.

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

8.5.1. the outcome of the test;

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

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

8.6. 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.

4.

9. Invoking the BCDR Plan

9.1. 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.

10. Circumstances beyond your control

10.1. 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.

4. PART B: ANNEX 1 Bespoke BCDR Plan

[**Guidance Note:** Where applicable, append the bespoke BCDR Plan.]

RM3808 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.]

1. 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: a) 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 b) 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

3.3. where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.

3.4. The references to standards, guidance and policies contained or set out in Paragraph The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which: 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.

3.5. 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:

a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;

b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

c) 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;

d) 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;

e) 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;

f) 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

g) 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 Amendment of the Security Management Plan, 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 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., or any subsequent revision to it in accordance with Paragraph Amendment of the Security Management Plan, 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 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. . 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 Content of the Security Management Plan shall be deemed to be reasonable.

4.3.4. Approval by the Buyer of the Security Management Plan pursuant to Paragraph 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. or of any change to the Security Management Plan in accordance with Paragraph Amendment of the Security Management Plan 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:

a) emerging changes in Good Industry Practice;

b) any change or proposed change to the Deliverables and/or associated processes;

c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;

d) any new perceived or changed security threats; and

e) 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;

b) updates to the risk assessments; and

c) suggested improvements in measuring the effectiveness of controls.

4.4.3. Subject to Paragraph 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., 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 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

4.4.4. 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 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., 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:

a) minimise the extent of actual or potential harm caused by any Breach of Security;

b) 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;

c) prevent an equivalent breach in the future exploiting the same cause failure; and

d) 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.

2. 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: a) 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 b) 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 I (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. [security representative of the Supplier - Edet.Umoren@colt.net]

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 The ISMS shall: to 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..

3.2. 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 Error: Reference source not found;

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

a) is in accordance with the Law and this Contract;

b) complies with the Baseline Security Requirements;

c) as a minimum demonstrates Good Industry Practice;

d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;

e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework);

f) takes account of guidance issued by the Centre for Protection of National Infrastructure (https://www.cpni.gov.uk/);

g) complies with HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm);

h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

i) addresses issues of incompatibility with the Supplier's own organisational security policies; and

j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph Error: Reference source not found;

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 The ISMS shall: 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 The ISMS shall:, 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 I 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 The ISMS shall: to 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. shall be deemed to be reasonable.

3.8. Approval by the Buyer of the ISMS pursuant to Paragraph 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. 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 Error: Reference source not found fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph The Security Management Plan shall:.

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 The ISMS shall:);

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 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. is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph The Security Management Plan shall: shall be deemed to be reasonable.

4.4. Approval by the Buyer of the Security Management Plan pursuant to Paragraph If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable. 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 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., 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 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:, a Buyer request, a change to Annex nnex 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 under-performance for the period of the Buyer's test.

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

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

a) minimise the extent of actual or potential harm caused by any Breach of Security;

b) 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;

c) 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;

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

e) 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

f) 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 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;

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 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: shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

3. 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 UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").

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 CESG End User Devices Platform Security Guidance (https://www.gov.uk/government/publications/end-user-device-strategy-security-framework-and-controls). 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 CESG 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 CESG, to at least Foundation Grade, for example, under CPA.

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 CESG Certified Professional certification (https://www.ncsc.gov.uk/articles/cesg-certification-ia-professionals-and-guidance-certification-ia-professionals-documents) 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.

8.1.3. The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

8.1.4. The Supplier shall retain audit records collected in compliance with this Paragraph Audit for a period of at least 6 Months.

4. PART B Annex 2: Security Management Plan

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.

1.2. Where the Buyer has not conducted a Further Competition Part B to this Schedule will apply.

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 Level"	means the actual level of performance of a Service achieved by the Supplier in relation to a Service Level Performance Criteria for a Service Period;
"Agreed Service Time"	means the period during which the Supplier ensures 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 Year"	means a consecutive period of twelve (12) Months commencing on the Call-Off Start Date or each anniversary thereof;
"Critical Service Level Failure"	takes the meaning; a) Specified by the Buyer where the Buyer selects Part A to this Call-Off Schedule 14; or b) any 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"	means any period of time within the Agreed Service Time during which a Service is not Available, excluding Planned Downtime;
"Imposed Carrier 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;

"Incident"	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;
"Incident Resolution Time"	means the time taken by the Supplier to Resolve an Incident, as set out in this Schedule;
"Planned Downtime"	means the time agreed in advance in writing by the Supplier and Buyer within the Agreed Service Time when a Service is not Available;
"Provisioning"	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;
"Resolution"	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 Credit Cap"	means: a) in the period from the Call-Off Start Date to the end of the first Call-Off Contract Year fifteen thousand pounds (£15,000); and b) during the remainder of the Call-Off Contract Period, thirty five per cent (35%) of the Call-Off Contract 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 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 b) 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 Desk"	means the single point of contact set up and operated by the Supplier to log, monitor and escalate Incidents, Incident Resolutions and Service Requests;
"Service Failure Threshold"	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;
"Service Level Failure"	means a failure to meet the Service Level Threshold in respect of a Service Level Performance Criterion;
"Service Level Performance Criteria"	means the criteria identified in either; a) Annex 1 to Part A of this Schedule; or b) paragraph 3.6 of Part B of this Schedule, against which the individual metrics are assessed; depending upon whether Part A or Part B is selected by the Buyer
"Service Levels"	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 Threshold"	shall be as set out against the relevant Service Level Performance Criteria in Annex 1 of Part A, or Annex 1 of Part B, of this Schedule depending upon which option is selected by the Buyer;
"Service Period"	means a recurrent period of one month during the Call-Off Contract Period, unless otherwise specified in the Order Form;
"Unavailable"	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:

a) exceeds the relevant Service Failure Threshold;

b) has arisen due to a Prohibited Act or wilful Default by the Supplier;

c) results in the corruption or loss of any Government Data; and/or

d) 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 otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 of the Core Terms (CCS and Buyer Termination Rights).

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 Critical Service Level Failure shall be without prejudice to the right of the Buyer to terminate this Contract pursuant to Clause 10.4 of the Core Terms (CCS and Buyer Termination Rights) and/or to claim damages from the Supplier for material Default.

1. 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 Level 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 Call-Off Schedule.

2. PART A Annex 1: Short Form Services Levels and Service Credits Table

[**Guidance Note:** The following are included by way of example only. Procurement-specific Service Levels should be incorporated]

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Threshold	Service Failure Threshold	
[Accurate and timely billing of Buyer]	**[Accuracy /Timelines]**	**Target time to repair service affecting faults is 8 hours**	**0-12 Hours**	**5% of monthly charge for 0-12 hours**
[Access to Buyer support]	**[Availability]**	**For Service affecting works, Customer will be notified at least ten (10) calendar days in advance for planned works.**	**[12 hours +**	**10% of monthly charge for 12 hours + The total of all credits under this SLA for services cannot exceed 40% of the annual rental charge for the affected Service.**

Critical Service Level Failure

[**Buyer Guidance:** Buyer to select from below.]

[Insert: Buyers required meaning for Critical Service Level Failure]

Service-Affecting Fault Any failure of our fibre, transmission or terminating Equipment, which causes full or partial loss of signals to the Customer's Service in one or both transmission directions.

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 payable by the Buyer
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)	=	23% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer]

3. 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:

a) 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

b) 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

c) 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

d) If a Critical Service Level Failure has occurred, exercise its right to compensation for such non-availability of Services via this Call-Off Contract.

3.4. 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.

3.5. The Buyer may enhance or otherwise modify the Service Levels required during a Further Competition Procedure.

3.6. 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:

3.6.1. Availability;

3.6.2. Incident Resolution;

3.6.3. Quality; and

3.6.4. 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:

4.4.

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:

$$\text{Achieved Availability \%} = \frac{(MP - SD) \times 100}{MP}$$

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:

$$\text{Achieved Incident Resolution \%} = \frac{(TI-FI) \times 100}{TI}$$

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 (%);

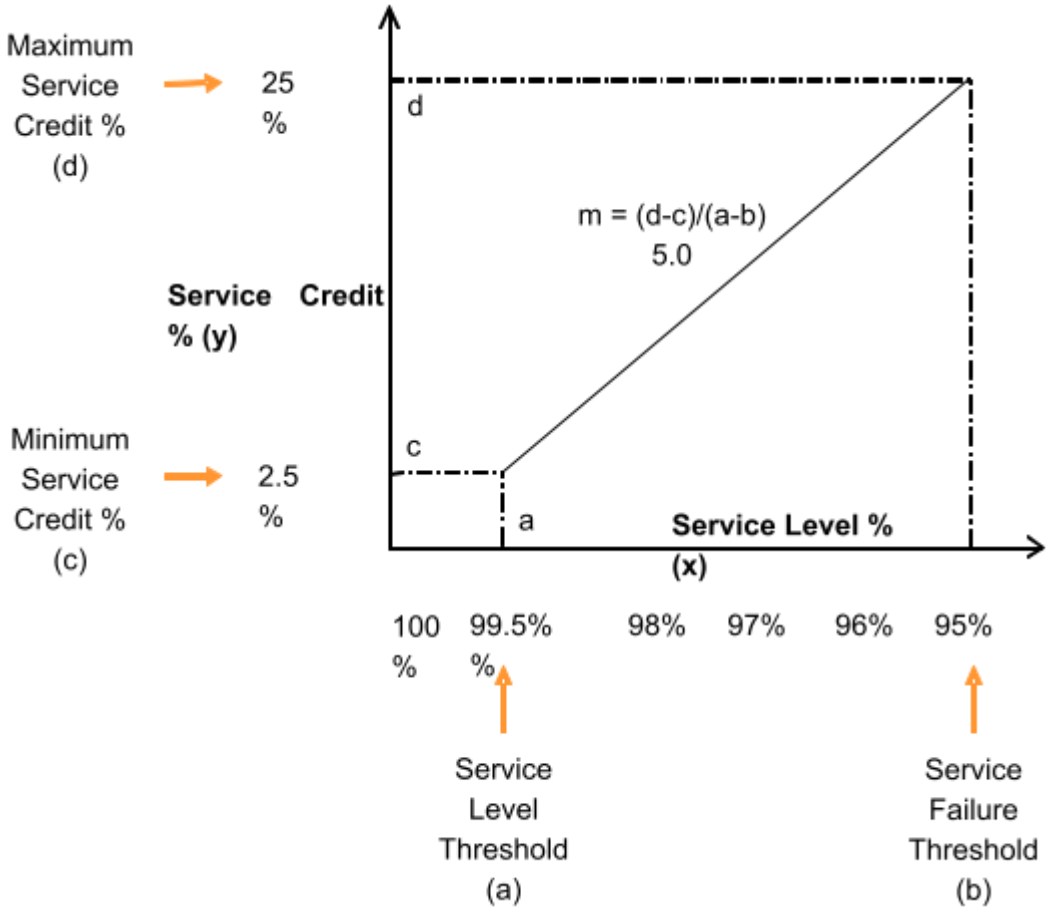
x is the Achieved Service Level Performance Criteria (%) for a Service Period;

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.

4. 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:

(a) The Services will only be deemed to have been Delivered once the Buyer has tested and accepted the quality of the data service;

(b) 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:

A. a fault is found, the Incident is Resolved as any other Incident;

B. 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:

(a) The Services will only be deemed to have been Delivered once the Buyer has tested and accepted the quality of the voice service;

(b) 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:

A. a fault is found, the Incident is Resolved as any other Incident;

B. 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.

5. 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.

6. 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 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. 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 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. of Part C of this Call-Off 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 (unless otherwise agreed):

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.]