

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

### Order Form

<b>CALL-OFF REFERENCE:</b>	PROC-884-2024
<b>THE BUYER:</b>	The Competition and Markets Authority
<b>BUYER ADDRESS</b>	Competition and Markets Authority The Cabot 25 Cabot Square London E14 4QZ7/ United Kingdom
<b>THE SUPPLIER:</b>	Insight Direct (UK) Ltd (the "Supplier")
<b>SUPPLIER ADDRESS:</b>	1st Floor, 1 St Paul's Place, Sheffield, S1 2JX
<b>REGISTRATION NUMBER:</b>	02579852
<b>DUNS NUMBER:</b>	769387739
<b>SID4GOV ID:</b>	208171
<b>SUPPLIER REF NUMBER</b>	18719
<b>CONTRACT SPECIALIST</b>	

### APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 10/02/2025.

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

### CALL-OFF LOT(S):

Lot 1 Hardware and Software and Associated Services

## **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 (Excluding Joint Schedules and Call-off Schedules)
2. Joint Schedule 1 (Definitions and Interpretation) RM6098
3. Framework Special Terms.
4. The following Schedules in equal order of precedence:
  - Joint Schedules for RM6098
    - Joint Schedule 2 (Variation Form)
    - Joint Schedule 3 (Insurance Requirements) – As appended to this Order Form (Appendix 1)
    - Joint Schedule 4 (Commercially Sensitive Information) – As appended to this Order Form (Appendix 2)
    - Joint Schedule 10 (Rectification Plan)
    - Joint Schedule 11 (Processing Data) – As appended to this Order Form (Appendix 3)
  - Call-Off Schedules for RM6098
    - Call-Off Schedule 5 (Pricing Details) – As appended to this Order Form (Appendix 4)
    - Call-Off Schedule 6 (ICT Services) – As appended to this Order Form (Appendix 5)
    - Call-Off Schedule 7 (Key Supplier Staff) – As appended to this Order Form (Appendix 6)
    - Call-Off Schedule 14 (Service Levels) – As appended to this Order Form (Appendix 7)
    - Call-Off Schedule 15 (Call-Off Contract Management) – As appended to this Order Form (Appendix 8)
    - Call-Off Schedule 20 (Call-Off Specification) – As appended to this Order Form (Appendix 9)
5. CCS Core Terms (version 3.0.11) as amended by the Framework Award Form
6. Joint Schedule 5 (Corporate Social Responsibility) RM6098
7. Call-Off Schedule 4 (Call-Off Tender) – As appended to this Order Form (Appendix 10). As long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery. For the avoidance of doubt, the contract provision shall only be defined by Call-Off Incorporated Terms 1 to 7 above and no other contract terms are applicable.

## **CALL-OFF SPECIAL TERMS**

The following Special Terms are incorporated into this Call-Off Contract:

The entirety of the following sections of Annex 3 within the CMA's Invitation to Tender, issued by the Buyer 05/08/2024:

- Annex 3, Section 5 (Information Security)
- Annex 3, Section 6 (Supplementary Terms and Conditions of Contract)
- Annex 3, Section 7 (Confidentiality and Security Requirements)
- Annex 3, Section 8 (Confidentiality Undertaking)
- Annex 3, Section 9 (Conflicts of Interest)

CALL-OFF START DATE: **11/02/2025**

CALL-OFF EXPIRY DATE: **10/02/2028**

CALL-OFF INITIAL PERIOD: **36 Months**

## **CALL-OFF DELIVERABLES**

As set out in Call-Off Schedule 20 (Call-Off Specification)

## **LOCATION FOR DELIVERY:**

TBS  
Competition and Markets Authority  
The Cabot  
25 Cabot Square  
London  
E14 4QZ  
United Kingdom

## **DATES FOR DELIVERY:**

## Software and Support

Both software and support are to be delivered on the Call-off Start Date.

## Hardware

Name	Category	Part Number	Quantity	Supplier Delivery Date
Cisco DNA Center Appliance (Gen 3) - 32 Core	Hardware	DN3-HW-APL	3	
Cisco ISE Small Secure Network Server Appliance	Hardware	SNS-3715-K9	2	
Cisco ISE Small Secure Network Server Appliance Storage Disk	Hardware	SNS-SD960GM2NK9	2	
Cisco Catalyst 9300X - Network Advantage - Replacing 3850 EoL	Hardware	C9300X-48TX-A	2	
Cisco Catalyst 9300X - 8x25/10/1Gbps Uplink Module	Hardware	C9300X-NM-8Y	2	
Cisco Catalyst 9300X - Additional Power Supply	Hardware	PWR-C1-715WAC-P	2	
Cisco Catalyst 9300X - StacWise cable	Hardware	Stack-T1-3M	2	

## TESTING OF DELIVERABLES

### Hardware

- i. All hardware will be tested for functionality on delivery.
- ii. This testing period will be 3 months from delivery of hardware.
- iii. The testing will be marked as successful if hardware is working and fully functional by the Buyer.

### Software and Support

N/A

## WARRANTY PERIOD

The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall be 90 days.

Framework Ref: RM6098  
 Project Version: v2.0  
 Model Version: v3.8

## **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 £283,686.32 (ex VAT).

## **CALL-OFF CHARGES**

Total call-off charges (Firm and Non-variable) for the 36-month Call-off Initial Period are as follows:

**Hardware:** [REDACTED]

**Licences:** [REDACTED]

**Support:** [REDACTED]

**Total Price: £571,113.48** (ex VAT)

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

## **REIMBURSABLE EXPENSES**

None

## **PAYMENT METHOD**

**All invoices submitted by the Supplier shall include the Buyer's Purchase Order reference, the invoicing period, the Services delivered within that period and the name of the Buyer's Authorised Representative.**

The following payment terms apply:

- Hardware will be paid within 30 days of receipt of goods, providing a valid invoice has already been sent to the Buyer. All hardware must be invoiced in one single document.
- Support and Licensing elements will be paid annually in advance, as detailed in Appendix 10 – Annex 8.

## **BUYER'S INVOICE ADDRESS:**

Accounts Payable

[REDACTED]

## **BUYER'S AUTHORISED REPRESENTATIVE**

[REDACTED]  
[REDACTED]  
[REDACTED]

**SUPPLIER'S AUTHORISED REPRESENTATIVE**

[REDACTED]  
[REDACTED]  
[REDACTED]

Insight Direct (UK) Ltd, 3 Hardman Street, 8th Floor, Manchester, M3 3HF

**SUPPLIER'S CONTRACT MANAGER**

[REDACTED]  
[REDACTED]  
[REDACTED]

Insight Direct (UK) Ltd, 3 Hardman Street, 8th Floor, Manchester, M3 3HF

**PROGRESS REPORT FREQUENCY**

On the first Working Day of each calendar month

**PROGRESS MEETING FREQUENCY**

During 1st year of the Call-Off Contract, the Supplier will attend monthly Progress Meetings. During Year 2 and 3 the Supplier will attend these meetings on a quarterly basis.

**KEY STAFF**

[REDACTED]  
[REDACTED]  
[REDACTED]

Insight Direct (UK) Ltd, 3 Hardman Street, 8th Floor, Manchester, M3 3HF

[REDACTED]

**KEY SUBCONTRACTOR(S)**

Not Applicable

**COMMERCIALLY SENSITIVE INFORMATION**

Not Applicable

**SERVICE CREDITS**

Not applicable

**ADDITIONAL INSURANCES**

Not applicable

[REDACTED]  
[REDACTED]  
[REDACTED]

**GUARANTEE**

Not applicable

**SOCIAL VALUE COMMITMENT**

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender) – Annex 6

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:		Signature:	
Name:		Name:	
Role:		Role:	
Date:	10/02/2025	Date:	7 <sup>th</sup> February 2025

## Appendix 1 - Joint Schedule 3 (Insurance Requirements)

### 1. The insurance you need to have:

- 1.1.1 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:
- 1.1.2 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
- 1.1.3 the Call-Off Contract Effective Date in respect of the Additional Insurances.

### 1.2 The Insurances shall be:

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

### 2. How to manage the insurance

- 2.1 Without limiting the other provisions of this Contract, the Supplier shall:
  - 2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;



- 2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
- 2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

### **3. What happens if you aren't insured**

- 3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.
- 3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

### **4. Evidence of insurance you must provide**

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

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

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

### **6. Cancelled Insurance**

- 6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or 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 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.
- 7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

## **ANNEX: REQUIRED INSURANCES**

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

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

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

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

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

## Appendix 2 - Joint Schedule 4 (Commercially Sensitive Information)

### 1. What is the Commercially Sensitive Information?

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

No.	Date	Item(s)	Duration of Confidentiality
18719	25/10/2024	1. Pricing breakdown 2. Technical Solutions	Five (5) Years

## Appendix 3 - Joint Schedule 11 (Processing Data)

### Definitions

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

<b>“Processor Personnel”</b>	All directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;
------------------------------	---

### Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

- (a) “Controller” in respect of the other Party who is “Processor”;
- (b) “Processor” in respect of the other Party who is “Controller”;
- (c) “Joint Controller” with the other Party;
- (d) “Independent Controller” of the Personal Data where the other Party is also “Controller”,

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

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

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 (*Processing Personal Data*) by the Controller and may not otherwise be determined by the Processor.
4. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

- (a) a systematic description of the envisaged Processing and the purpose of the Processing;
  - (b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
  - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
  - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
- (a) Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*) and shall not Process the Personal Data for any other purpose, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
  - (b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protection Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take account of the:
    - (i) nature of the data to be protected;
    - (ii) harm that might result from a Data Loss Event;
    - (iii) state of technological development; and
    - (iv) cost of implementing any measures;
  - (c) ensure that:
    - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
    - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
      - (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;
      - (B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

- (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
  - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
- (d) not transfer, Process, or otherwise make available for Processing, Personal Data outside of the UK unless the prior written consent of the Controller has been obtained (such consent may be withheld or subject to such conditions as the Customer considers fit at the Customer's absolute discretion) and the following conditions are fulfilled:
  - (i) the destination country has been recognised as adequate by the UK Government in accordance with Article 45 UK GDPR or section 74 of the DPA 2018;
  - (ii) Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 DPA 2018) as determined by the Controller;
  - (iii) the Data Subject has enforceable rights and effective legal remedies;
  - (iv) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
  - (v) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data;

if any of the mechanisms relied on under paragraph 6(d) in respect of any transfers of Personal Data by the Processor at any time ceases to be valid, the Processor shall, if possible, implement an alternative mechanism to ensure compliance with the Data Protection Legislation. If no alternative mechanism is available, the Controller and the Processor shall work together in good faith to determine the appropriate measures to be taken, taking into account any relevant guidance and accepted good industry practice. The Controller reserves the right to require the Processor to cease any affected transfers if no alternative mechanism to ensure compliance with Data Protection Legislation is reasonably available; and
- (e) at the written direction, and absolute discretion, of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of

the Contract unless the Processor is required by Law to retain the Personal Data.

7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to Processing Personal Data under or in connection with the Contract it:
  - (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
  - (b) receives a request to rectify, block or erase any Personal Data;
  - (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
  - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
  - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
  - (f) becomes aware of a Data Loss Event.
8. The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
9. Taking into account the nature of the Processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
  - (a) the Controller with full details and copies of the complaint, communication or request;
  - (b) such assistance as is requested by the Controller to enable the Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
  - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
  - (d) assistance as requested by the Controller following any Data Loss Event; and/or
  - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.



10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
  - (a) the Controller determines that the Processing is not occasional;
  - (b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
  - (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
13. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
  - (a) notify the Controller in writing of the intended Subprocessor and Processing that will be undertaken by the Subprocessor;
  - (b) obtain the written consent of the Controller (such consent may be withheld or subject to such conditions as the Controller considers fit at the Controller's absolute discretion);
  - (c) enter into a written legally binding agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor, prior to any Personal Data being transferred to or accessed by the Subprocessor; and
  - (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
14. Any Processing by a Subprocessor or transfer of Personal Data to a Subprocessor permitted by the Controller shall not relieve the Processor from any of its liabilities, responsibilities and obligations to the Controller under this Joint Schedule 11, and the Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).
16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30)

Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

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

17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 3 to this Joint Schedule 11.

### **Independent Controllers of Personal Data**

18. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
19. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
22. The Parties shall only provide Personal Data to each other:
  - (a) to the extent necessary to perform their respective obligations under the Contract;
  - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
  - (c) where it has recorded it in Annex 1 (*Processing Personal Data*).
23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the

requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):
  - (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
  - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
    - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
    - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
26. Each Party shall promptly notify the other Party upon it becoming aware of any Data Loss Event relating to Personal Data provided by the other Party pursuant to the Contract and shall:
  - (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Data Loss Event;
  - (b) implement any measures necessary to restore the security of any compromised Personal Data;
  - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
  - (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

27. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (*Processing Personal Data*).
28. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).
29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 28 of this Joint Schedule 11.

## Annex 1 - Processing Personal Data

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

1. The contact details of the Relevant Authority's Data Protection Officer are: [REDACTED]
2. The contact details of the Supplier's Data Protection Officer are: [REDACTED]
3. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
4. Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	<p><b>The Relevant Authority is Controller and the Supplier is Processor</b></p> <p>The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"> <li>• CMA staff's Personal Data (which may include sensitive data for certain agreed services), Personal Information of visitors</li> <li>• Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller,</li> </ul>
Duration of the Processing	The Framework Contract Period and thereafter, until expiry or termination of the last Call-Off Contract under the Framework, including the period until all transactions relating to Call-Off Contracts have permanently ceased
Nature and purposes of the Processing	<p>The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</p> <p>The purpose might include: estate, asset &amp; property management, agency &amp; lease management, survey &amp; strategic advice, project management, valuation, business rating services, operational &amp; strategic workplace</p>

	<p>management.</p> <p>To facilitate the procurement of Goods and Services from the Framework Contract by public sector organisations and enable CCS to provide ongoing support and a point of escalation for CMA in the day-to-day management of their individual Call-Off Contracts.</p> <p>Day to day management and performance of obligations under the Framework Contract, including exit management and other associated activities.</p>
Type of Personal Data	<p>Categories of Personal data required for the performance of the potentially contracted activities specified under 'nature and purposes of processing':</p> <ul style="list-style-type: none"> <li>• Personal Information including but not limited to: Name, Work Email, Job title, Work Phone number, Work address, Image, Sensitive data such as accident and injury or health related data</li> <li>• Protected information as defined in Equality Act</li> </ul>
Categories of Data Subject	<p>Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc</p> <p>Personnel data of the Parties involved in the performance of obligations and day to day management of the Contract.</p>
<p>Plan for return and destruction of the data once the Processing is complete</p> <p>UNLESS requirement under Union or Member State law to preserve that type of data</p>	<p>Data will be retained for seven (7) years after the duration of the processing outlined above and in accordance with the CCS Privacy Notice.</p> <p>In accordance with the Core Terms, all CCS data and any copies held by the Supplier must be securely erased once the Processing is complete, unless the Supplier is required by law to retain it.</p> <p>In accordance with the Core Terms, all Storage Media that has held CCS data must be securely destroyed at the end of life of the media. All destruction of media must be in line with good industry practice.</p>

## Annex 2 – Security

The technical security requirements set out below provide an indication of the types of security measures that might be considered, in order to protect Personal Data. More, or less, measures may be appropriate depending on the subject matter of the contract, but the overall approach must be proportionate. The technical requirements must also be compliant with legislative and regulatory obligations for content and data, such as UK GDPR. The example technical security requirements set out here are intended to supplement, not replace, security schedules that will detail the total contractual security obligations and requirements that the Processor (i.e. a supplier)

will be held to account to deliver under contract. Processors are also required to ensure sufficient 'flow-down' of legislative and regulatory obligations to any third party Sub-processors.

**External Certifications e.g.** Buyers should ensure that Suppliers hold at least Cyber Essentials certification and ISO 27001:2013 certification if proportionate to the service being procured.

**Risk Assessment e.g.** Supplier should perform a technical information risk assessment on the service supplied and be able to demonstrate what controls are in place to address those risks.

**Security Classification of Information e.g.** If the provision of the Services requires the Supplier to Process Authority/Buyer Data which is classified as OFFICIAL, OFFICIAL-SENSITIVE or Personal Data, the Supplier shall implement such additional measures as agreed with the Authority/Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable legislative and regulatory obligations.

**End User Devices e.g.**

- The Supplier shall ensure that any Authority/Buyer Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority/Buyer except where the Authority/Buyer has given its prior written consent to an alternative arrangement.
- The Supplier shall ensure that any device which is used to Process Authority/Buyer Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security>.

**Testing e.g.** The Supplier shall at their own cost and expense, procure a CHECK or CREST Certified Supplier to perform an ITHC or Penetration Test prior to any live Authority/Buyer data being transferred into their systems. The ITHC scope must be agreed with the Authority/Buyer to ensure it covers all the relevant parts of the system that processes, stores or hosts Authority/Buyer data.

**Networking e.g.** The Supplier shall ensure that any Authority/Buyer Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

**Personnel Security e.g.** All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard or

equivalent including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. The Supplier may be required to implement additional security vetting for some roles.

**Identity, Authentication and Access Control e.g.** The Supplier must operate an appropriate access control regime to ensure that users and administrators of the service are uniquely identified. The Supplier must retain records of access to the physical sites and to the service.

**Data Destruction/Deletion e.g.** The Supplier must be able to demonstrate they can supply a copy of all data on request or at termination of the service, and must be able to securely erase or destroy all data and media that the Authority/Buyer data has been stored and processed on.

**Audit and Protective Monitoring e.g.** The Supplier shall collect audit records which relate to security events in delivery of the service 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 regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority/Buyer Data. The retention periods for audit records and event logs must be agreed with the Authority/Buyer and documented.

**Location of Authority/Buyer Data e.g.** The Supplier shall not, and shall procure that none of its Sub-contractors, process Authority/Buyer Data outside the EEA without the prior written consent of the Authority/Buyer and the Supplier shall not change where it or any of its Sub-contractors process Authority/Buyer Data without the Authority/Buyer's prior written consent which may be subject to conditions.

**Vulnerabilities and Corrective Action e.g.** Suppliers shall procure and implement security patches to vulnerabilities in accordance with the timescales specified in the NCSC Cloud Security Principle 5.

Suppliers must ensure that all COTS Software and Third Party COTS Software be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support.

**Secure Architecture e.g.** Suppliers should design the service in accordance with:

- NCSC "[Security Design Principles for Digital Services](#)"
- NCSC "[Bulk Data Principles](#)"
- NCSC "[Cloud Security Principles](#)"



## **Annex 3 - Joint Controller Agreement**

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

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 3 (Joint Controller Agreement) in replacement of paragraphs 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 18-28 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the Supplier:

- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
- (b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- (c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
- (d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and
- (e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the Supplier's privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

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

### **2. Undertakings of both Parties**

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

- (a) report to the other Party every 3 months on:

- (i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
- (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
- (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
- (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
- (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

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

- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
- (e) request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

- (g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
  - (i) are aware of and comply with their duties under this Annex 3 (Joint Controller Agreement) and those in respect of Confidential Information;
  - (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
  - (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
- (h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:
  - (i) nature of the data to be protected;
  - (ii) harm that might result from a Data Loss Event;
  - (iii) state of technological development; and
  - (iv) cost of implementing any measures;
- (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and
- (j) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

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

### **3. Data Protection Breach**

3.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming

aware of any Data Loss Event or circumstances that are likely to give rise to a Data Loss Event, providing the other Party and its advisors with:

- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Data Loss Event under the Data Protection Legislation; and
- (b) all reasonable assistance, including:
  - (i) co-operation with the other Party and the Information Commissioner investigating the Data Loss Event and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
  - (ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Data Loss Event;
  - (iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Data Loss Event; and/or
  - (iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Data Loss Event, with complete information relating to the Data Loss Event, including, without limitation, the information set out in Clause 3.2.

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

- (a) the nature of the Data Loss Event;
- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Data Loss Event; and
- (f) describe the likely consequences of the Data Loss Event.

#### **4. Audit**

##### **4.1 The Supplier shall permit:**

- (a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 3 and the Data Protection Legislation; and/or
- (b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

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

#### **5. Impact Assessments**

##### **5.1 The Parties shall:**

- (a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and
- (b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

#### **6. ICO Guidance**

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

#### **7. Liabilities for Data Protection Breach**

- 7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Data Loss Event ("**Financial Penalties**") then the following shall occur:
- (a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Data Loss Event, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Data Loss Event. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Data Loss Event;
  - (b) if in the view of the Information Commissioner, the Supplier is responsible for the Data Loss Event, in that it is not a Data Loss Event that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Data Loss Event; or
  - (c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Data Loss Event and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Data Loss Event can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).
- 7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Data Loss Event, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Data Loss Event shall be liable for the losses arising from such Data Loss Event. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.
- 7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Data Loss Event (the "Claim Losses"):
- (a) if the Relevant Authority is responsible for the relevant Data Loss Event, then the Relevant Authority shall be responsible for the Claim Losses;

- (b) if the Supplier is responsible for the relevant Data Loss Event, then the Supplier shall be responsible for the Claim Losses: and
- (c) if responsibility for the relevant Data Loss Event is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

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

## **8. Termination**

If the Supplier is in material Default under any of its obligations under this Annex 3 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

## **9. Sub-Processing**

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

- (a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
- (b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

## **10. Data Retention**

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

Appendix 4 - Call-Off Schedule 5 (Pricing Details)

All costs within this schedule are firm, non-variable and ex VAT.

Hardware

Name	Part Number	Quantity	Price per Unit	Total Price
------	-------------	----------	----------------	-------------



License Name	SKU	Start Date	End Date	Quantity	Price per Licence	Total Price

[illegible]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

### Support

Part Number	Serial Number	Device Description	Start Date	End Date	Required New Support Level Cisco Direct Support Model	Price per Support Element
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[illegible]

[illegible]

**Call-Off Schedule 5 (Call-Off Pricing)**  
Crown Copyright 2017

[illegible]

[illegible]

[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>
<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>
<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>
<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>
<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>
<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>
<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>
<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>
<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>



### **Maximum Margin for Additional Contract Provisions**

When the Buyer informs the Supplier of additional purchases through this contract, the following margins will be the maximum addition percentage cost applied to the base pricing by the Supplier for central government organisations:

Cost Category	Maximum Margin
Hardware	
Licences	
Support	

## Appendix 5 - Call-Off Schedule 6 (ICT Services)

### 1. Definitions

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

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

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or

c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or

d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;

### **"Emergency Maintenance"**

ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;

### **"ICT Environment"**

the Buyer System and the Supplier System;

### **"Licensed Software"**

all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;

### **"Maintenance Schedule"**

has the meaning given to it in paragraph 8 of this Schedule;

<b>"Malicious Software"</b>	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
<b>"New Release"</b>	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
<b>"Open Source Software"</b>	computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;
<b>"Operating Environment"</b>	<p>means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which:</p> <ul style="list-style-type: none"><li>a) the Deliverables are (or are to be) provided; or</li><li>b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or</li><li>c) where any part of the Supplier System is situated;</li></ul>

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

Call-Off Ref:

Crown Copyright 2018

<b>"Permitted Maintenance"</b>	has the meaning given to it in paragraph 8.2 of this Schedule;
<b>"Quality Plans"</b>	has the meaning given to it in paragraph 6.1 of this Schedule;
<b>"Sites"</b>	has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;
<b>"Software"</b>	Specially Written Software COTS Software and non-COTS Supplier and third party Software;
<b>"Software Supporting Materials"</b>	has the meaning given to it in paragraph 9.1 of this Schedule;
<b>"Source Code"</b>	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
<b>"Specially Written Software"</b>	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;

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

Call-Off Ref:

Crown Copyright 2018

### **"Supplier System"**

the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

## **2. When this Schedule should be used**

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

## **3. Buyer due diligence requirements**

3.1. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;

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

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

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

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

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

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

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

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

Call-Off Ref:

Crown Copyright 2018

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

## **4. Licensed software warranty**

4.1. The Supplier represents and warrants that:

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

4.1.2. all components of the Specially Written Software shall:

4.1.2.1. be free from material design and programming errors;

4.1.2.2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels) and Documentation; and

4.1.2.3. not infringe any IPR.

## **5. Provision of ICT Services**

5.1. The Supplier shall:

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

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

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

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

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

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

## 6. Standards and Quality Requirements

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

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

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

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

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

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

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



## **7. ICT Audit**

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

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

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

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

## **8. Maintenance of the ICT Environment**

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

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

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

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

## 9. Intellectual Property Rights in ICT

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

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

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

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

9.1.2. The Supplier shall:

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

9.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and

9.1.2.3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that

any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

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

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

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

- a) of its own Existing IPR that is not COTS Software;
- b) third party software that is not COTS Software

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

9.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

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

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

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

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

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

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

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

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

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

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

9.3.4.2. will no longer be made commercially available

#### **9.4. Buyer's right to assign/novate licences**

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

9.4.1.1. a Central Government Body; or

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

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

#### **9.5. Licence granted by the Buyer**

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

#### **9.6. Open Source Publication**

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

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

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

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

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

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

running or security of the Specially Written Software, New IPRs or the Buyer System;

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

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

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

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

9.6.2.6. do not contain any Malicious Software.

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

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

9.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software

and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

### **9.7. Malicious Software**

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

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

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

9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

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

## Appendix 6 - Call-Off Schedule 7 (Key Supplier Staff)

- 1.1 The Order Form lists the key roles ("**Key Roles**") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.
- 1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.
- 1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.
- 1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:
  - 1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
  - 1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or
  - 1.4.3 the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.
- 1.5 The Supplier shall:
  - 1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);
  - 1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
  - 1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least three (3) Months' notice;
  - 1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work



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

Call-Off Ref:

Crown Copyright 2018

- together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and
- 1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.
- 1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

## Appendix 7 - Call-Off Schedule 14 (Service Levels)

### 1. Definitions

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

<b>"Critical Service Level Failure"</b>	has the meaning given to it in the Order Form;
<b>"Service Credits"</b>	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;
<b>"Service Credit Cap"</b>	has the meaning given to it in the Order Form;
<b>"Service Level Failure"</b>	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
<b>"Service Level Performance Measure"</b>	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
<b>"Service Level Threshold"</b>	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

### 2. What happens if you don't meet the Service Levels:

- 2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.
- 2.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Performance Measure.
- 2.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- 2.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:
  - 2.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or
  - 2.4.2 the Service Level Failure:
    - (a) exceeds the relevant Service Level 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
  - 2.4.3 the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).
- 2.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:
  - 2.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;
  - 2.5.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and
  - 2.5.3 there is no change to the Service Credit Cap.

### 3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

- 3.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and
- 3.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"),  
provided that the operation of this paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

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

### **1. Service Levels**

If the level of performance of the Supplier:

- 1.1 is likely to or fails to meet any Service Level Performance Measure; or
- 1.2 is likely to cause or causes a Critical Service Failure to occur,

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

- 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 to Part A of this Schedule.

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

Service Levels				Service Credit for each Service Period	
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold		Publishable KPI
Hardware Delivery	Timescales	Time Taken to Deliver Hardware to The CMA After Order Confirmation from The Supplier			No
Requests for Quotation	Timescales	Time Taken for The Supplier to Provide a Quotation After Request from the CMA			No
Additional Orders	Timescales	Time Taken to Confirm Additional Orders After Request from CMA			No

## Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

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

Number of instances per Service Level Performance Criterion x Service Credit for each Service Period	=	x% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer
--	---	---

Worked example: 4 instances of tardiness over all SLAs x 0.5%	=	2% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer
--	---	---

## Part B: Performance Monitoring

### 3. Performance Monitoring and Performance Review

- 3.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.
- 3.2 The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the process and timescales agreed pursuant to paragraph 1.1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:
  - 3.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;
  - 3.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;
  - 3.2.3 details of any Critical Service Level Failures;
  - 3.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;
  - 3.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and
  - 3.2.6 such other details as the Buyer may reasonably require from time to time.
- 3.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:
  - 3.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;
  - 3.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and
  - 3.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant

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

Call-Off Ref:

Crown Copyright 2018

meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.

- 3.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.
- 3.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

**4. Satisfaction Surveys**

- 4.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.



## **Appendix 8 - Call-Off Schedule 15 (Call-Off Contract Management)**

### **1. Definitions**

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

<b>"Operational Board"</b>	the board established in accordance with paragraph 4.1 of this Schedule;
<b>"Project Manager"</b>	the manager appointed in accordance with paragraph 2.1 of this Schedule;

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

Call-Off Ref:

Crown Copyright 2018

### **2. Project Management**

- 2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.
- 2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.
- 2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

### **3. Role of the Supplier Contract Manager**

- 3.1 The Supplier's Contract Manager's shall be:
  - 3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;
  - 3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;
  - 3.1.3 able to cancel any delegation and recommence the position himself; and
  - 3.1.4 replaced only after the Buyer has received notification of the proposed change.
- 3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager's in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.
- 3.3 Receipt of communication from the Supplier's Contract Manager's by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

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

Call-Off Ref:

Crown Copyright 2018

### **4. Role of the Operational Board**

- 4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.
- 4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.
- 4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.
- 4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.
- 4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

### **5. Contract Risk Management**

- 5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.
- 5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:
  - 5.2.1 the identification and management of risks;
  - 5.2.2 the identification and management of issues; and
  - 5.2.3 monitoring and controlling project plans.
- 5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.
- 5.4 The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer's and the Supplier have identified.

## **Annex: Contract Boards**

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

During the first year of the contract, the Supplier will attend these meetings monthly.

During the second and third year of the contract the Supplier will attend these meetings on a quarterly basis.

Three (3) months prior to the contract expiry date the Supplier shall attend a meeting to discuss the end of the contract. In this meeting the Supplier will provide a renewal quote for all active Cisco services to the CMA.

These boards will primarily be held via Teams, if there is a need for a site visit this must be agreed by the Buyer in advance.

## **Appendix 9 - Call-Off Schedule 20 (Call-Off Specification)**

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

### **1 OBJECTIVES AND OUTPUT**

The objective of this procurement is to procure a Cisco Partner for licensing, support and Hardware. This Cisco partner will:

- Help enrol into the Cisco Enterprise Agreement for Licensing
- Provide co-terminated, direct Cisco TAC support solution for CMA's estate of hardware and software solutions.
- Provide hardware necessary to carry out Cisco DNA Center and Cisco ISE refresh.
- Provide network switch stack replacement.
- Provide Cisco Firepower Management Center hardware's alternative solution, delivered as Cloud native.

### **2 THE REQUIREMENT**

The below outlines the CMA's requirement for the Cisco Partner:

#### **2.1. Cisco Partner Requirements**

2.1.1. The Supplier shall have Cisco Gold Partnership Status.

2.1.2. The Supplier shall be an authorised Cisco reseller.

2.1.3. The Supplier shall provide an account manager who will be a single point of contract for:

- Contract queries
- Conflict resolution
- Adding additional provisions to the contract

#### **2.2. Supplier Contract Management**

2.2.1. The Supplier will be required to attend meetings to cover:

- Licensing and support plan management, including additions, true-ups and/or true-downs.
- Hardware support additions to main co-terminated support plan.
- Assist with new hardware deployment requirement planning.
- Assist with end of life (EOL) hardware tracking.

2.2.2. During 1st year of the contract, the Supplier will attend these meetings on a monthly basis.

2.2.3. During Year 2 and 3 the Supplier will attend these meetings on a quarterly basis.

2.2.4. Three (3) months prior to the contract expiry date the Supplier shall attend a meeting to discuss the end of the contract. In this meeting the Supplier will provide a renewal quote for all active Cisco services to the CMA.

2.2.5. During the contract term if there are any contract changes, this will be formalised by either party completing a contract Variation Form detailing any change, with any necessary supporting evidence.

2.2.6. Once both parties have signed this schedule these changes will form part of the contract.

### **2.3. Licensing:**

2.3.1. The Supplier will provide all licenses detailed within Annex A.

2.3.2. The Cisco licensing enterprise agreement within this contract will be co-termed to the contract end date.

2.3.3. The Supplier shall credit/transfer all current CMA current licensing solutions and use this credit towards the new Cisco Enterprise Agreement licensing model.

### **2.4. Support:**

2.4.1. The Supplier will provide all support elements within Annex B.

2.4.2. The CMA requires that all support communication is to be direct with Cisco TAC.

2.4.3. All support agreements within this contract will be co-termed to the contract end date.

### **2.5. Hardware:**

2.5.1. The Supplier shall provide all hardware within Annex C within the CMA's target lead times.

2.5.2. If any tenderer cannot provide the hardware within the target lead times within Annex C their tender response will be classed as invalid and the supplier will be disqualified.

#### **2.5.3. Delivery**

2.5.3.1. Hardware is to be delivered to:

Technology and Business services (TBS),  
The Competition and Markets Authority,  
25 Cabot Square,  
London,  
E14 4QZ

## **2.6. Period**

2.6.1. The core term of the contract will be 36 months.

## **2.7. Additional Provisions**

2.7.1. The Supplier shall provide the option to purchase additional network licenses, additional support plans and additional hardware during the term of the contract.

2.7.2. Any additional licenses or support elements purchased through the term of the contract will be co-termed to the contract end date.

2.7.3. Any additional purchases during the term of the contract will be managed via a Contract Variation Form.

2.7.4. The CMA reserves the right to purchase additional hardware from other suppliers where the value of the basket is over £25,000.

## **2.8. Pricing**

2.8.1. The initial contract purchase will consist of a firm total price for all provisions submitted in Appendix 4 - Call-Off Schedule 5 (Pricing Details).

2.8.2. The Supplier should provide a full transparent breakdown in the event that the CMA purchases additional provisions for goods and services through this contract.

2.8.2.1. This breakdown should include;

- Base costs and Margin of Licenses and Support
- Cost of hardware

2.8.3. Any additional provisions requested through the life of the contract will be held to the individual firm margins for software, hardware and support submitted in Annex 5 – Pricing Response Document.

## **2.9. Payments**

2.9.1. Hardware will be paid for on receipt of goods.

2.9.2. Support contract will be paid in full upon setup.

2.9.3. Annual payments will be made for licenses.

2.9.4. Invoices must include a valid Purchase Order and full breakdown of charges.

### **3 SERVICE LEVELS and KEY PERFORMANCE INDICATORS (KPIs)**

#### **3.1. SLAs**

3.1.1. The Supplier will make all reasonable efforts to deliver hardware at soonest time possible. However, delivery lead times should no later than 180 days from the date the order is place.

3.1.2. The Supplier will process requests for quotation of additional purchases within 1 week (7 days) of the request.

3.1.3. The Supplier will process additional orders within 1 week (7 days) of the request.

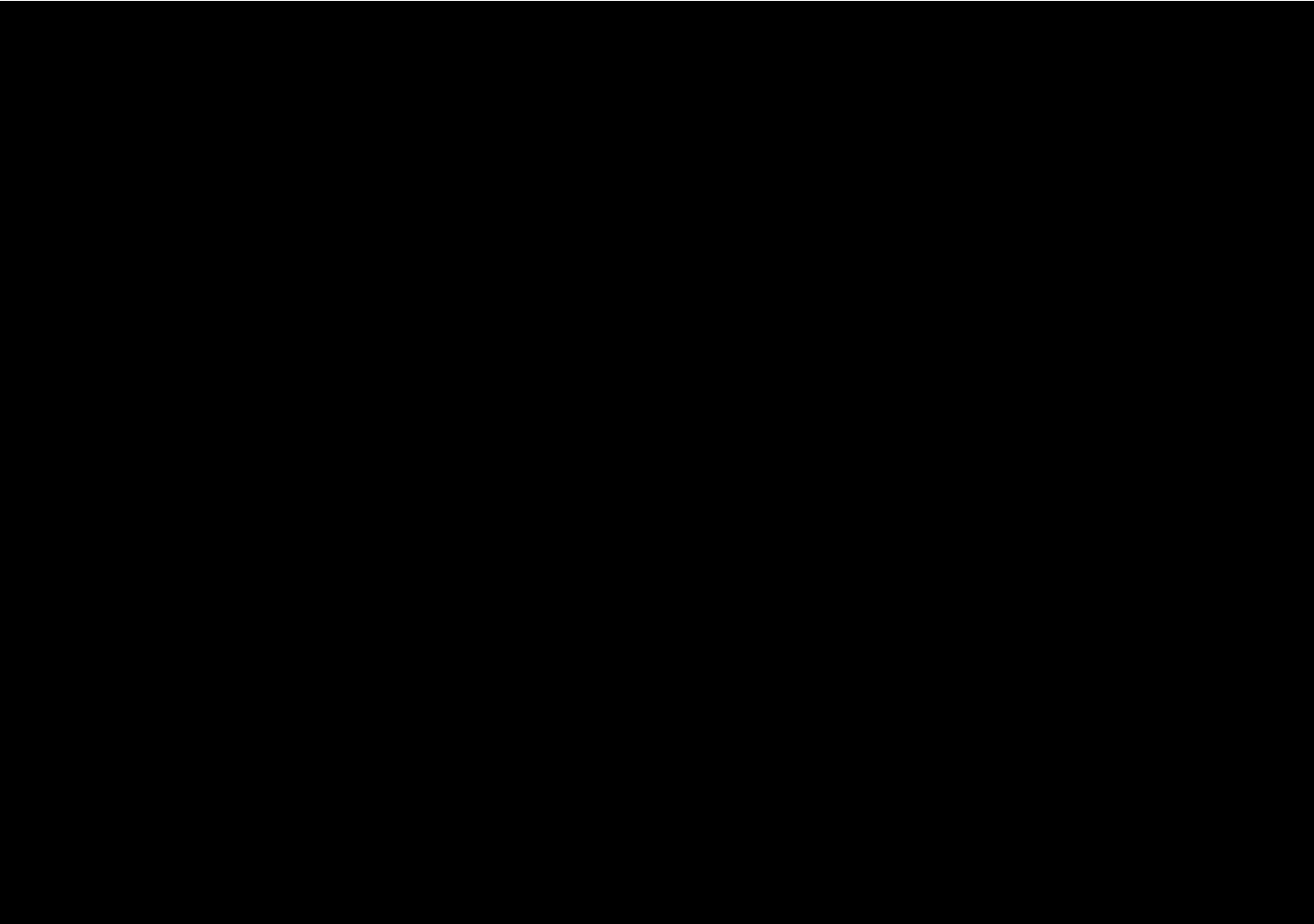
3.1.4. The Supplier will provide yearly summary report for End of Life, End of Support hardware and solutions.



Crown Copyright 2018

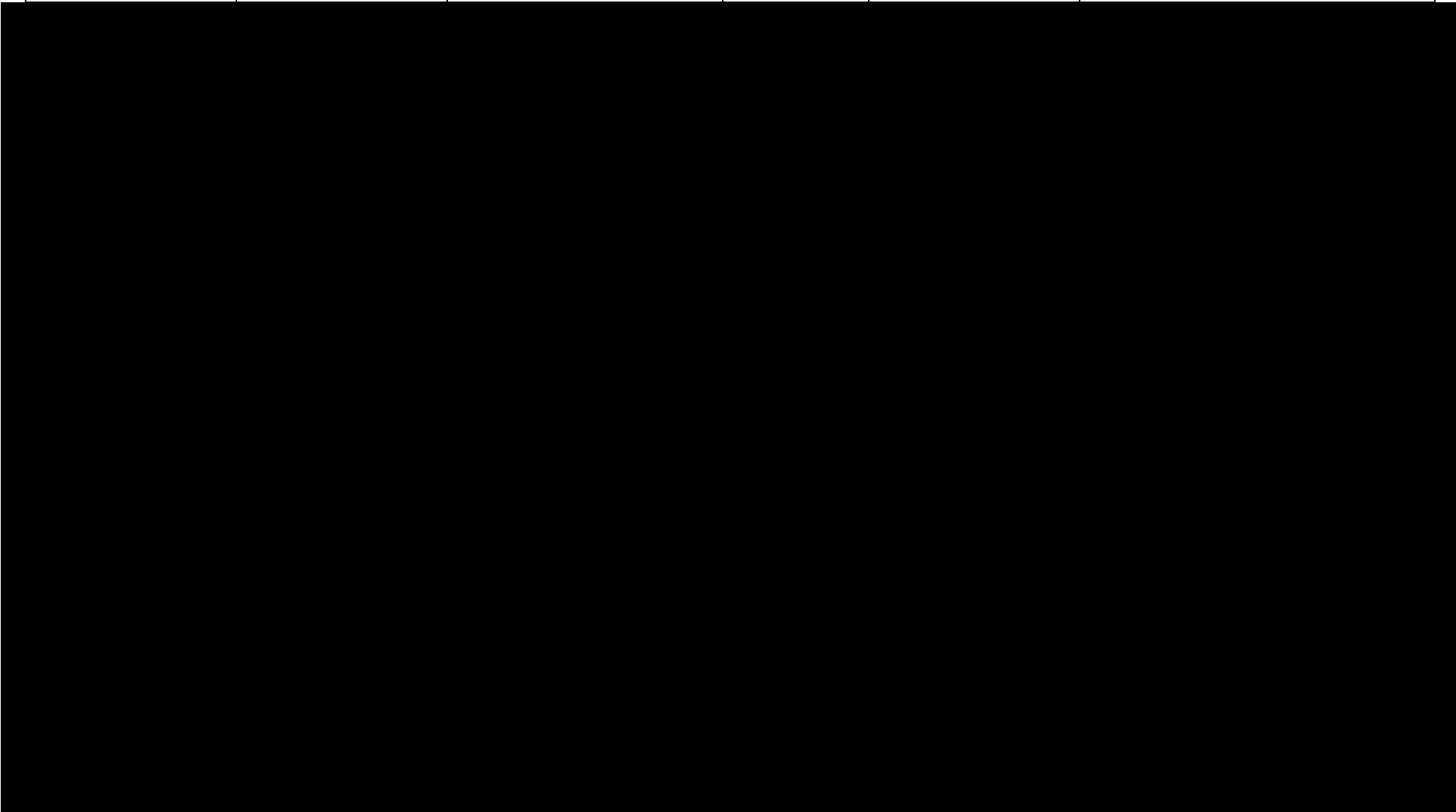
License Name	SKU	Current Count	Comment
--------------	-----	---------------	---------

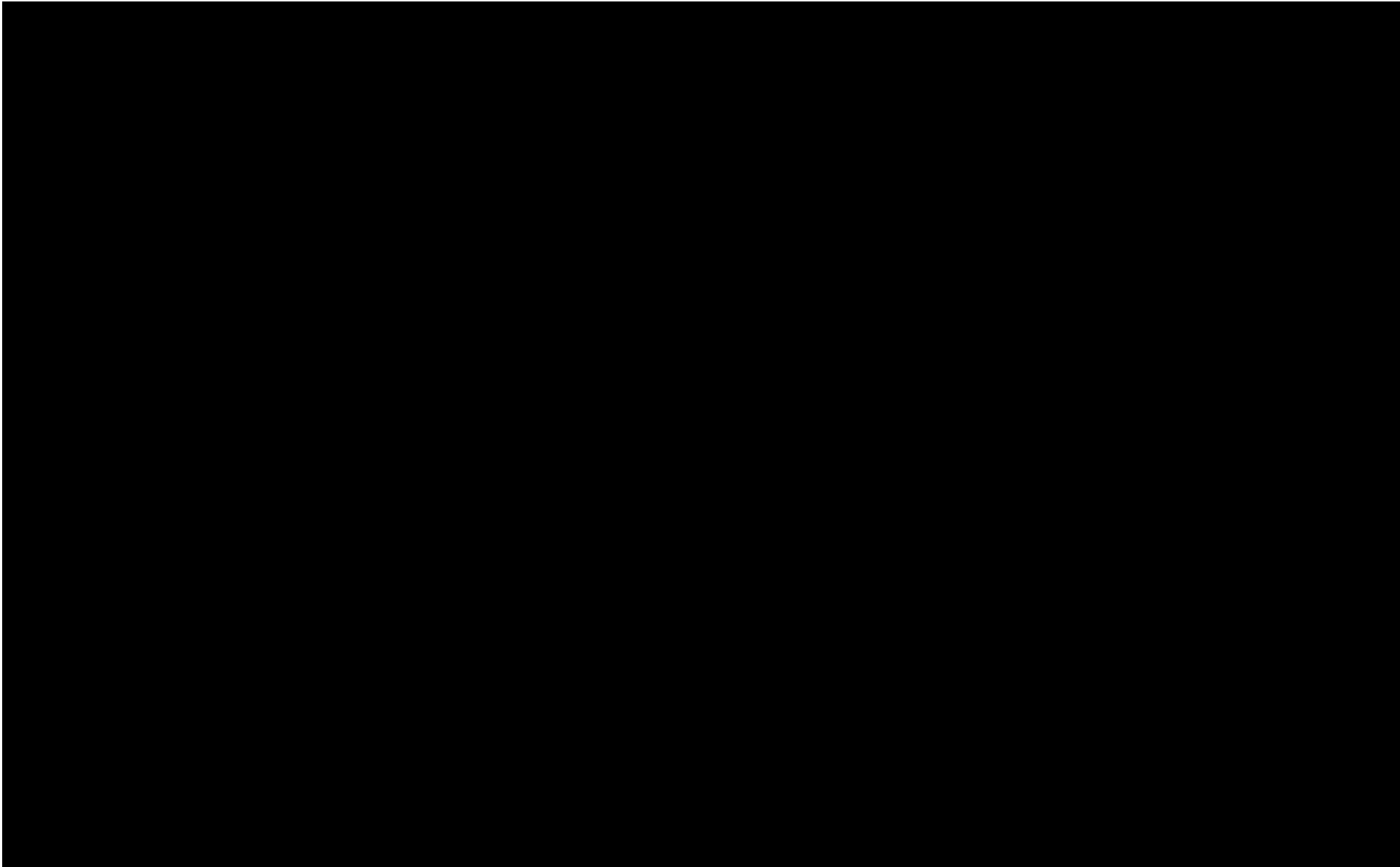
1. *Journal of the American Medical Association*, 1997; 277: 103-107.

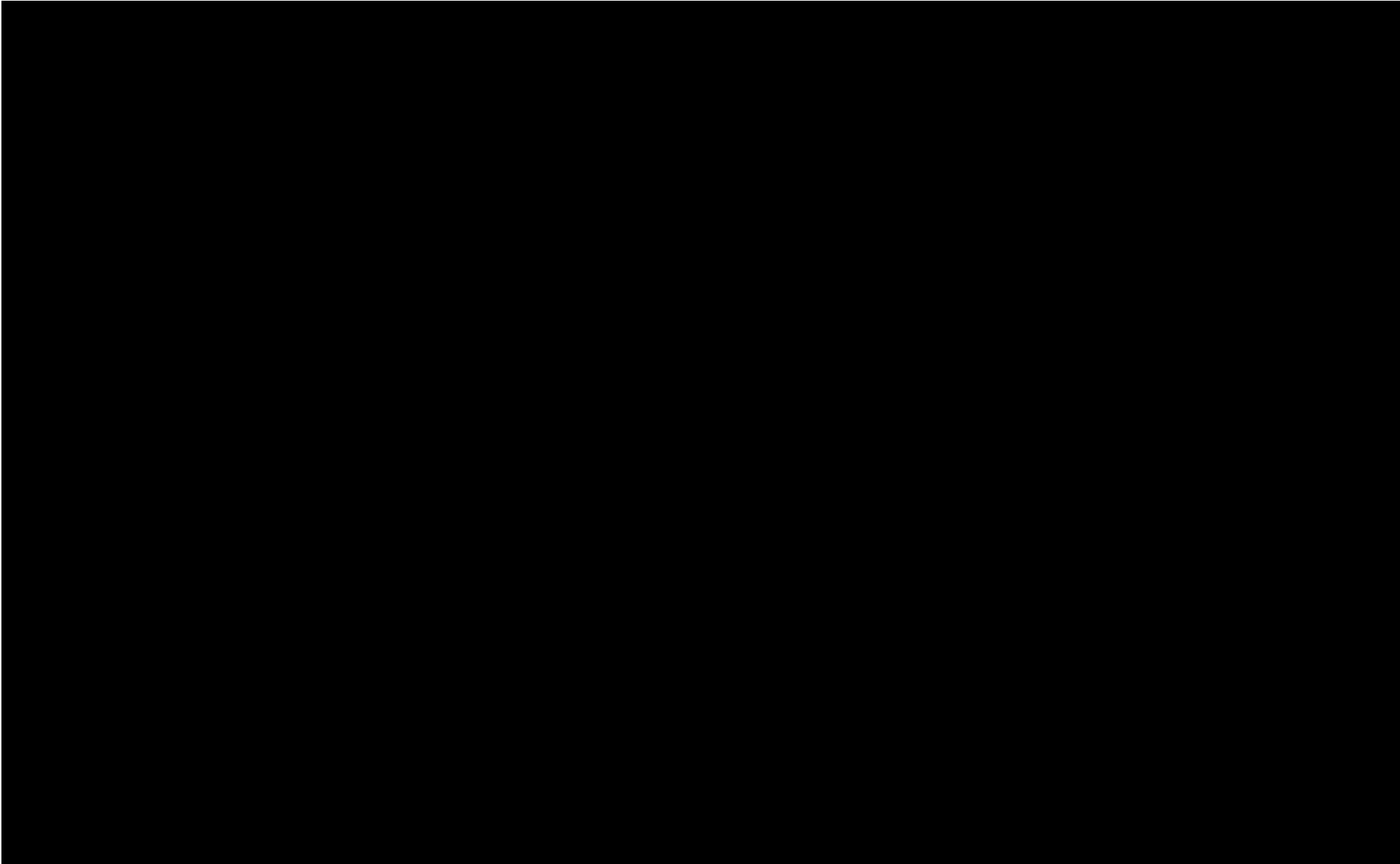


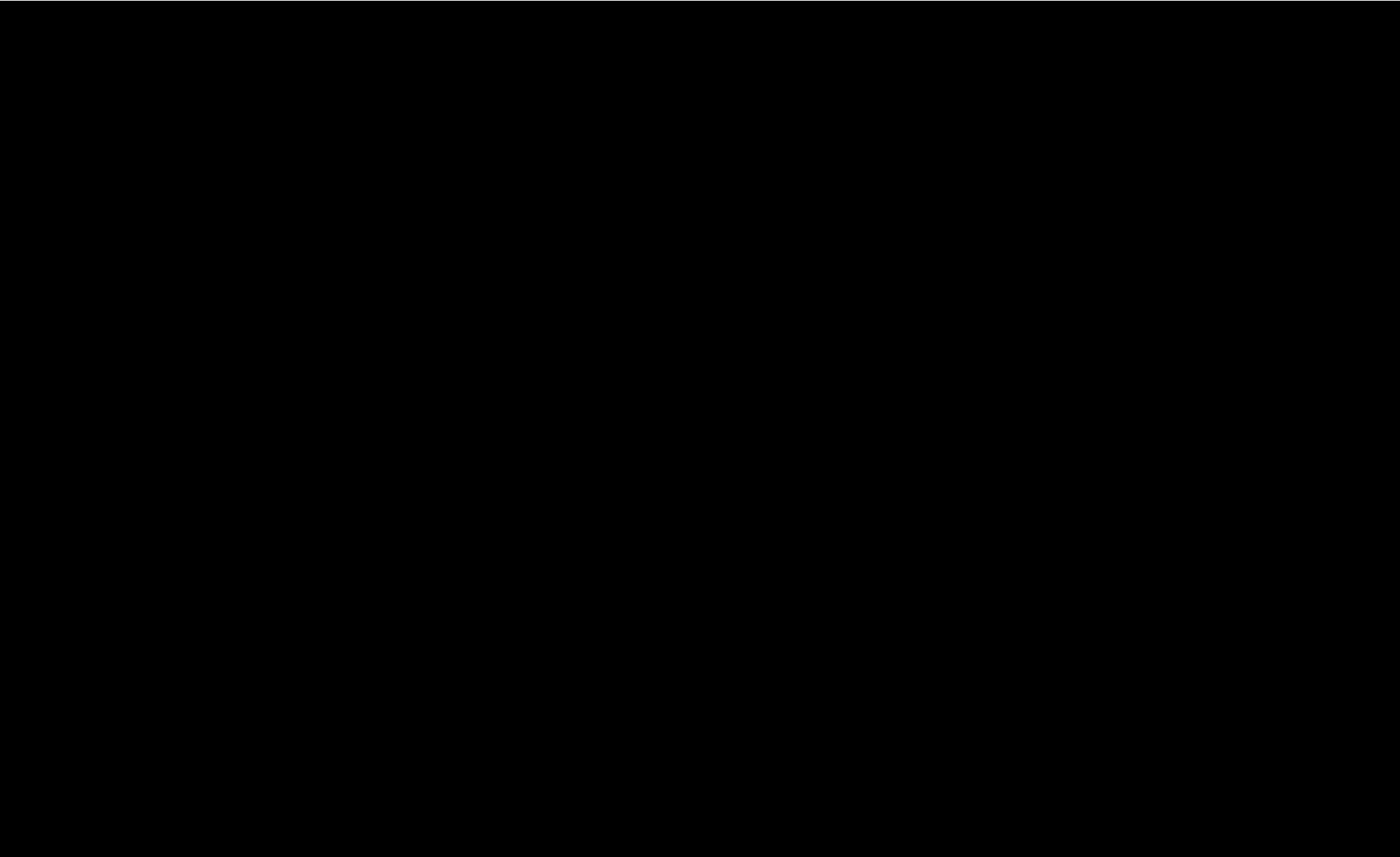
Call-Off Schedule 20 (Call-Off Specification)  
Call-Off Ref:  
Crown Copyright 2018

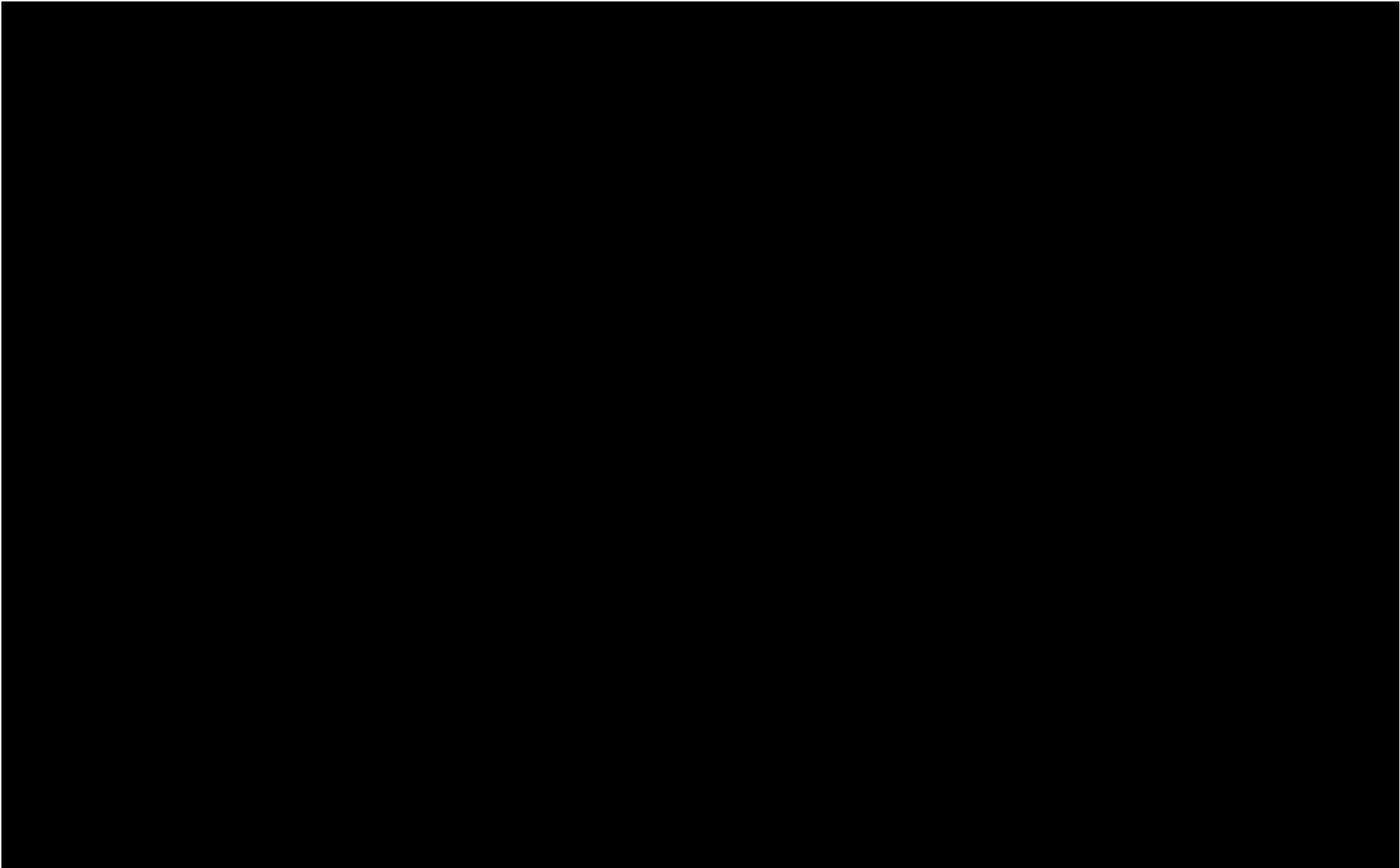
Part Number	Serial Number	Device Description	Current Support End Date	Current Supplier	Required New Support Level Cisco Direct Support Model
-------------	---------------	--------------------	--------------------------	------------------	---

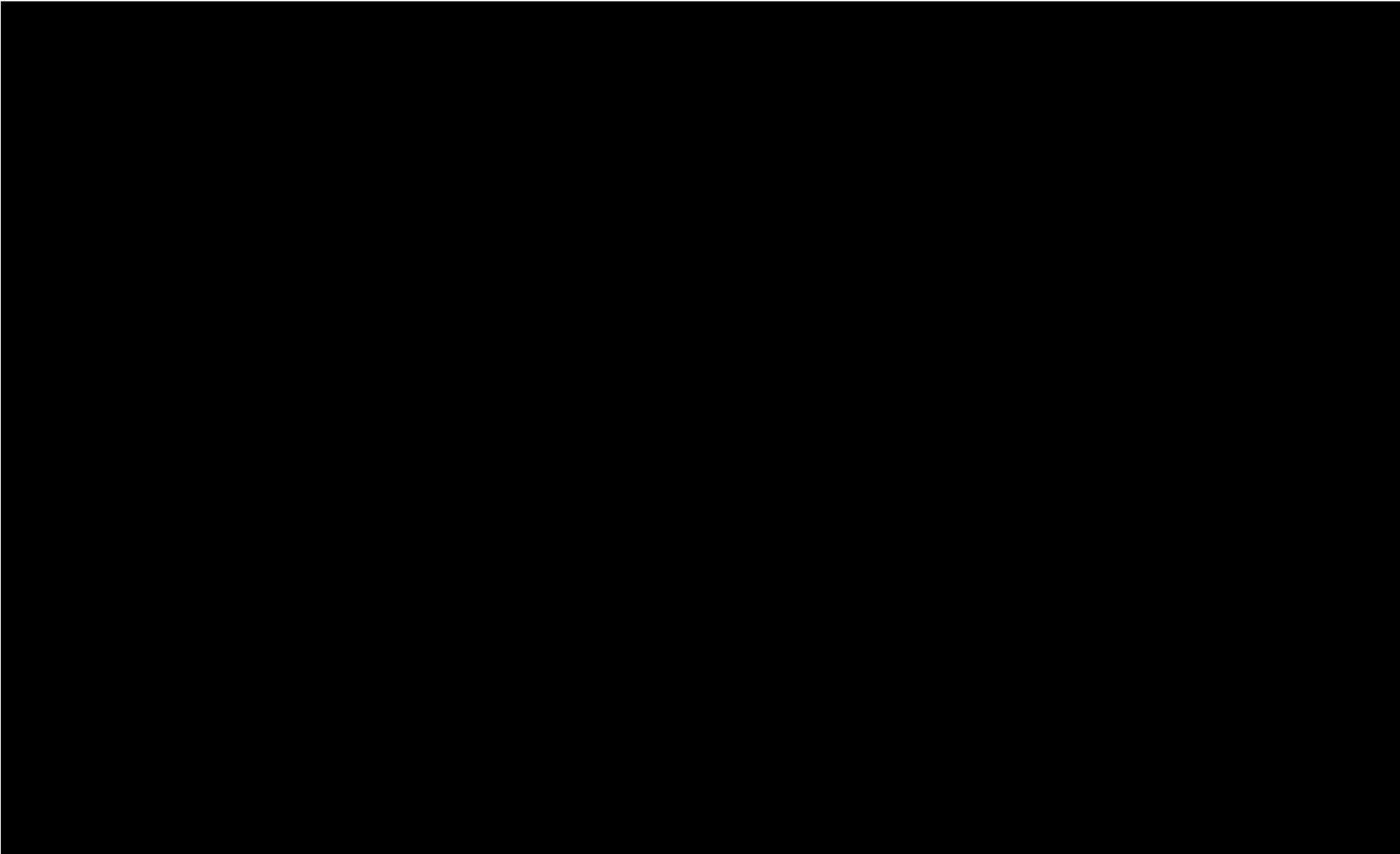




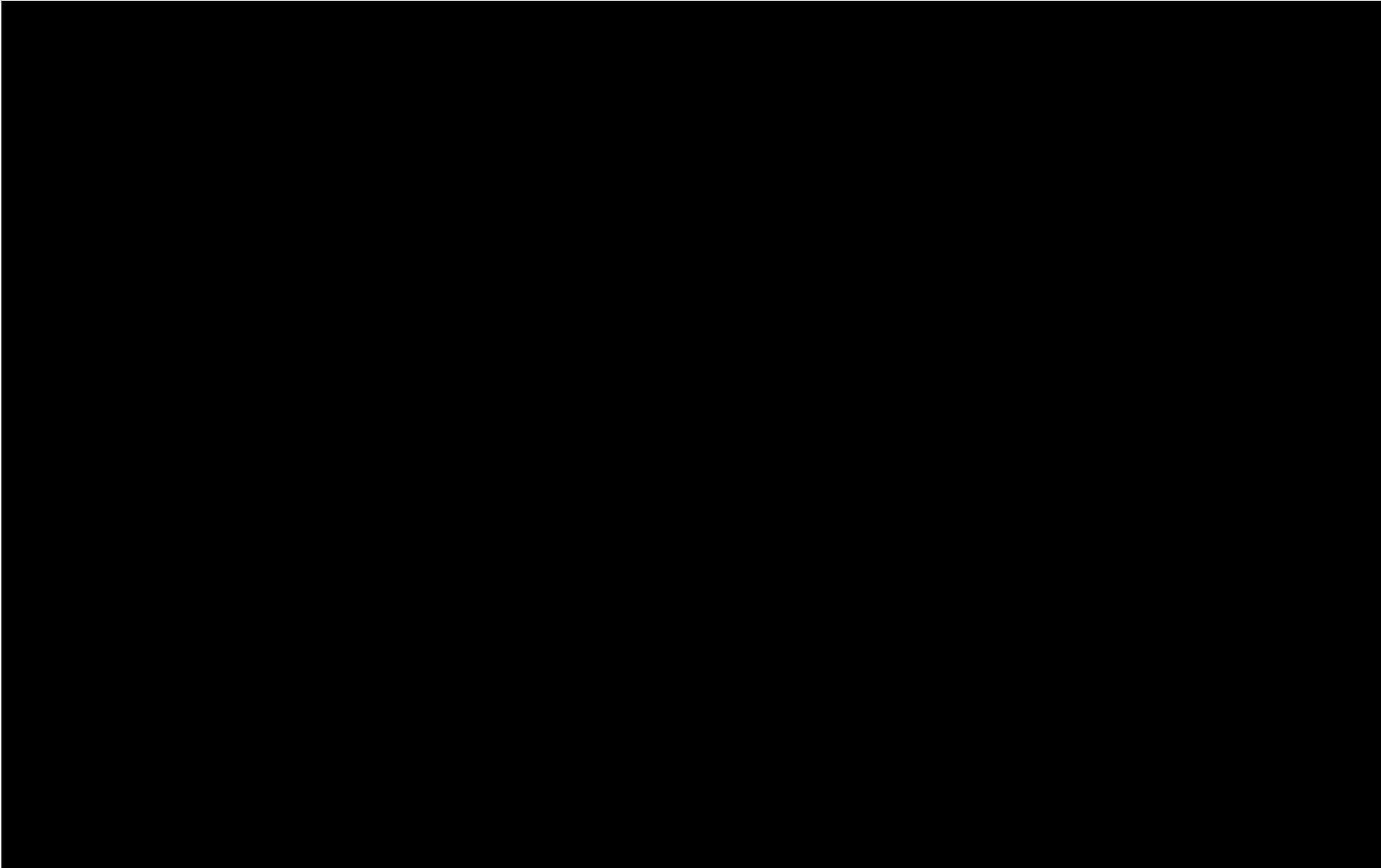


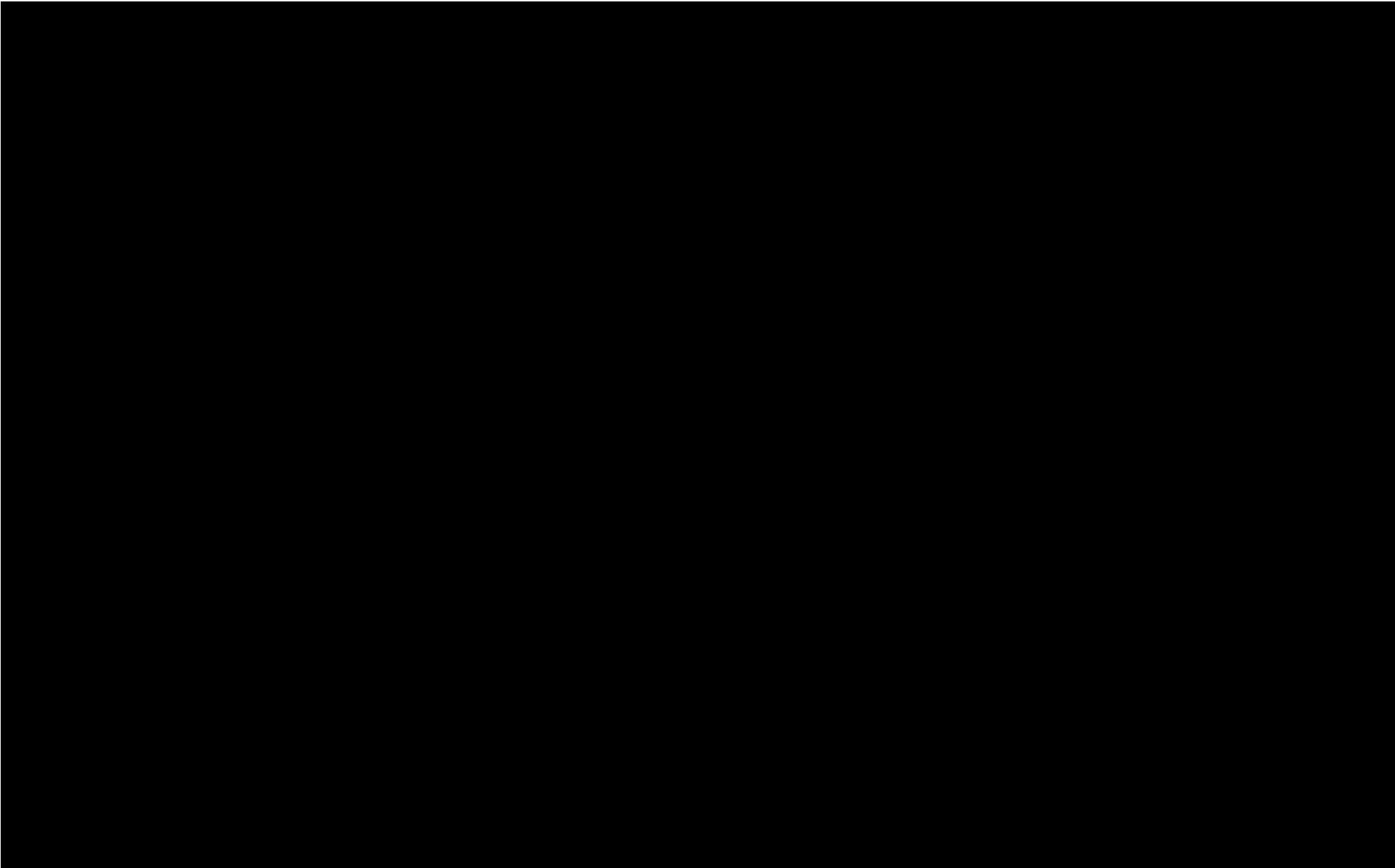


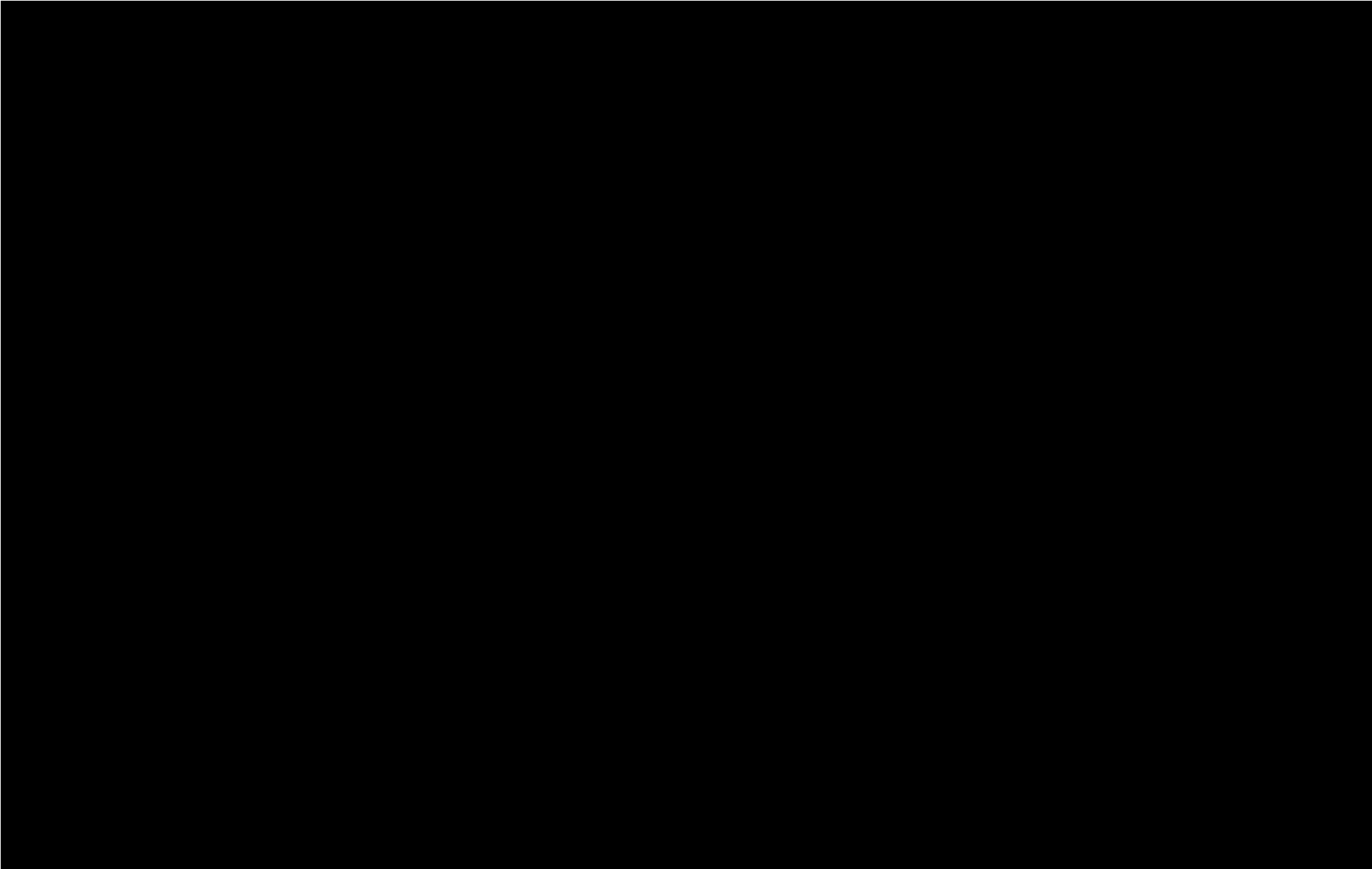




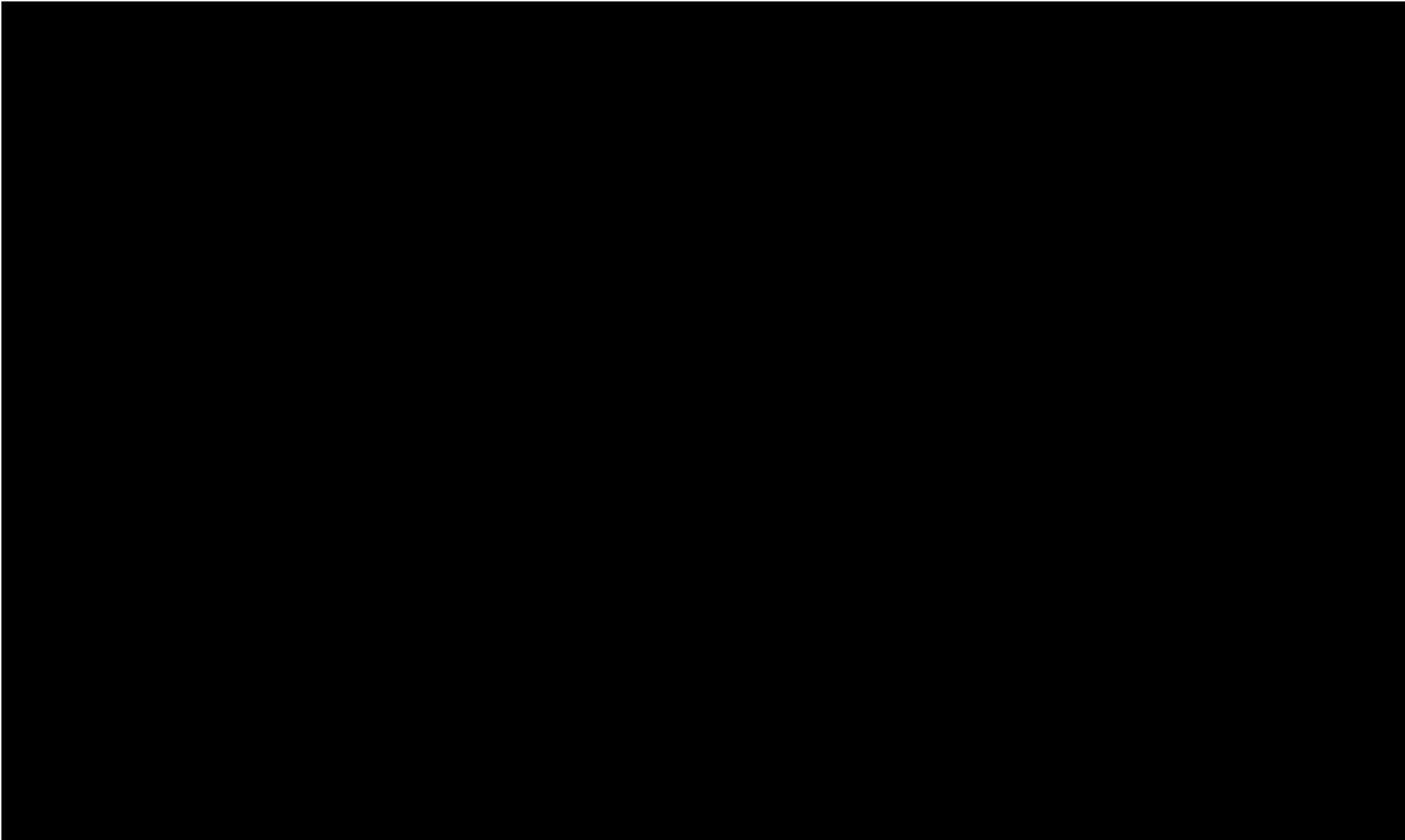


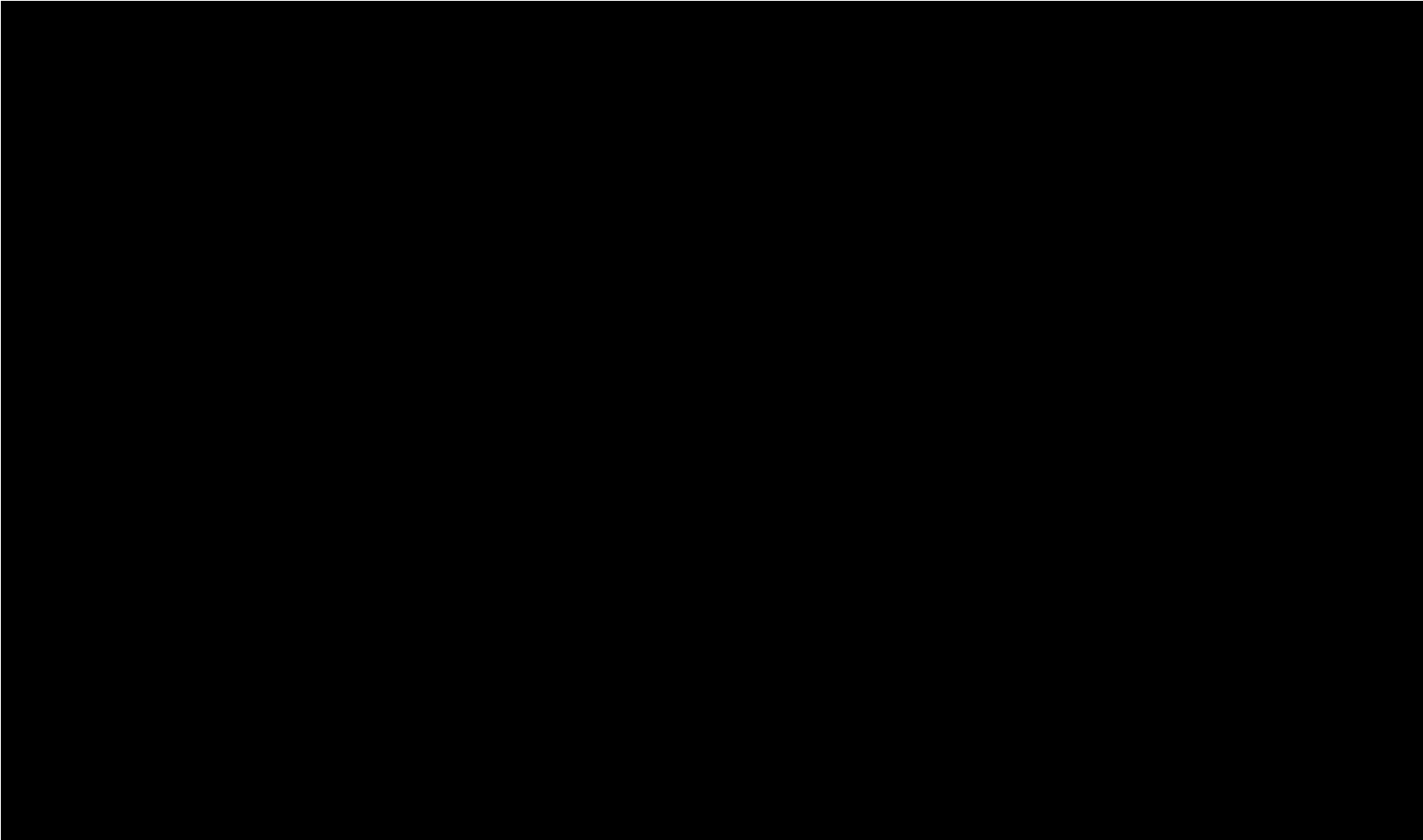


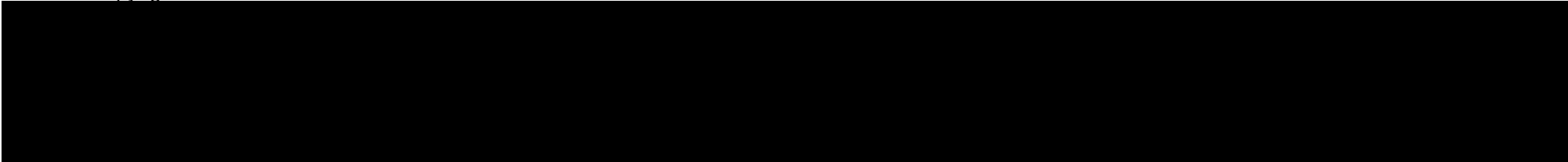












**Annex C – Hardware Specifications**

Name	Category	Expected to be delivered to CMA	Part Number	Quantity
------	----------	------------------------------------	-------------	----------

--	--	--	--	--



## **Appendix 10 - Call-Off Schedule 4 (Call Off Tender)**

### **Annex 1 – Stage 1, Compliance & Data Handling (Insight’s Response to Annex 3 of the ITT)**

Tenderers are required to complete and compile the additional twelve (12) sections and then submit these with their completed bids.

**Contract reference: Provision of a Cisco Partner**

**Procurement Reference: PROC-884-2024**

Please note completion of all elements of this section are mandatory, failure to complete a question or submit information may result in a non-compliant tender.

Bidders are required to complete and return this document along with any other supporting documentation by uploading to the attachments tab via the opportunity within the Delta Portal.

**STAGE 1: Mandatory Compliance**

1. General Compliance
2. Supplier Information
3. Form of Agreement
4. Certificate of Bona Fide Tendering
5. Information Security
6. Supplementary Terms and Conditions of Contract
7. Confidentiality and Security Requirements
8. Confidentiality Undertaking
9. Conflicts of Interest
10. Data Handling Assessment

**General Compliance**

Please confirm you agree to all the following statements by confirming Y/N and signing the below:

Category	Question	Confirm Yes or No
Compliance with the Specification	If you are awarded the call off contract, will you unreservedly deliver in full, all the deliverables as set out in Specification and all associated annexes.	Yes
Compliance with Attachment 5 (Order Form and additional schedules)	If you are awarded the call off contract, will you unreservedly deliver in full, all the deliverables as set out in the Specification and all associated schedules/ annexes.	Yes

**Response guidance**

The above are pass/fail questions. If you cannot or are unwilling to select 'yes' to these questions, you will be disqualified from further participation in this competition. Please confirm you agree to all the following statements by signing the below

<b>Minimum Pass Mark:</b>	Completion
<b>Fail</b>	Information supplied is missing, incomplete or unqualified
<b>Pass</b>	Information supplied is complete and qualified
<b>Your Response</b>	

**STAGE 1: Compliance & Data Handling**

1. General Compliance
2. Supplier Information
3. Form of Agreement
4. Certificate of Bona Fide Tendering
5. Information Security
6. Supplementary Terms and Conditions of Contract
7. Confidentiality and Security Requirements
8. Confidentiality Undertaking
9. Conflicts of Interest
10. Data Handling Assessment

<b>Supplier Information</b>	
Please complete the below information regarding the company bidding.	
<b>Minimum Pass Mark:</b>	Completion
<b>Fail</b>	Information supplied is missing, incomplete or unqualified
<b>Pass</b>	Information supplied is complete and qualified

Question number	Question	Your Response
1(a)	Full name of the Person submitting the information	
1(b) – (i)	Registered office address (if applicable)	
1(b) – (ii)	Registered website address (if applicable)	
1(c)	Trading status a) public limited company b) limited company c) limited liability partnership d) other partnership e) sole trader f) third sector g) other (please specify your trading status)	
1(d)	Date of registration in country of origin	
1(e)	Company registration number (if applicable)	
1(f)	Charity registration number (if applicable)	
1(g)	Head office DUNS number (if applicable)	
1(h)	Registered VAT number (if applicable)	
1(i) - (i)	If applicable, is your organisation registered with the appropriate professional or trade register(s) in the member state where it is established?	

Question number	Question	Your Response
1(i) - (ii)	If you responded yes to 1.1(i) - (i), please provide the relevant details, including the registration number(s).	
1(j) - (i)	Is it a legal requirement in the state where you are established for you to possess a particular authorisation, or be a member of a particular organisation in order to provide the services specified in this Procurement?	
1(j) - (ii)	If you responded yes to 1.1(j) - (i), please provide additional details of what is required and confirmation that you have complied with this.	
1(k)	Trading name(s) that will be used if successful in this Procurement	
1(l)	Relevant classifications (state whether you fall within one of these, and if so which one) a) Voluntary Community Social Enterprise (VCSE) b) Sheltered Workshop c) Public service mutual	
1(m)	Are you a Small, Medium or Micro Enterprise (SME) <sup>1</sup> ?	

<sup>1</sup> See EU definition of SME [https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition\\_en](https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en)

- I declare that to the best of my knowledge the answers submitted and information contained in this document are correct and accurate.
- I declare that, upon request and without delay I will provide the certificates or documentary evidence referred to in this document.
- I understand that the information will be used in the selection process to assess my organisation's suitability to be invited to participate further in this Procurement.
- I understand that the Authority may reject this Tender in its entirety if there is a failure to answer all the relevant questions fully, or if false/misleading information or content is provided in any section.

I am aware of the consequences of serious misrepresentation

Question number	Question	Your Response
1C.1(n)	Contact name	
1C.1(o)	Name of organisation	
1C.1(p)	Role in organisation	
1C.1(q)	Phone number	
1C.1(r)	E-mail address	

Call-Off Schedule 20 (Call-Off Specification)

Call-Off Ref:

Crown Copyright 2018

Question number	Question	Your Response
1C.1(s)	Postal address	
1C.1(t)	Signature	
1C.1(u)	Date	

**STAGE 1: Compliance & Data Handling**

1. General Compliance
2. Supplier Information
3. **Form of Agreement**
4. Certificate of Bona Fide Tendering
5. Information Security
6. Supplementary Terms and Conditions of Contract
7. Confidentiality and Security Requirements
8. Confidentiality Undertaking
9. Conflicts of Interest
10. Data Handling Assessment

FORM OF AGREEMENT	
Your Response	
To	The CMA, The Cabot, 25 Cabot Square, London E14 4QZ
Date	07/08/2024
<p><b>INVITATION TO TENDER PROC REF, PROC 884-2024</b></p> <p>I have examined the proposed Contract documents consisting of: Form of Agreement and Certificate of Bona Fide Tendering; Terms and Conditions of Contract; Statement of Requirement; Schedule of Rates and Prices; Tender Terms and Conditions and ITT Special Notices and Instructions to Tenderers.</p> <p>I hereby offer to enter into a Contract with the Authority upon the Conditions in the proposed Contract documents and for the Rates and Prices entered in the enclosed Schedule of Rates and Prices. Pricing information is valid for 90 days from the submission date.</p> <p>I warrant that I have all the requisite corporate authority to sign this tender.</p> <p>I have completed and appended the "Certificate of Bona Fide Tendering".</p> <p>I understand that the Authority is not bound to accept the lowest or any Tender.</p>	
Minimum Pass Mark:	Completion
Fail	Information supplied is missing, incomplete or unqualified

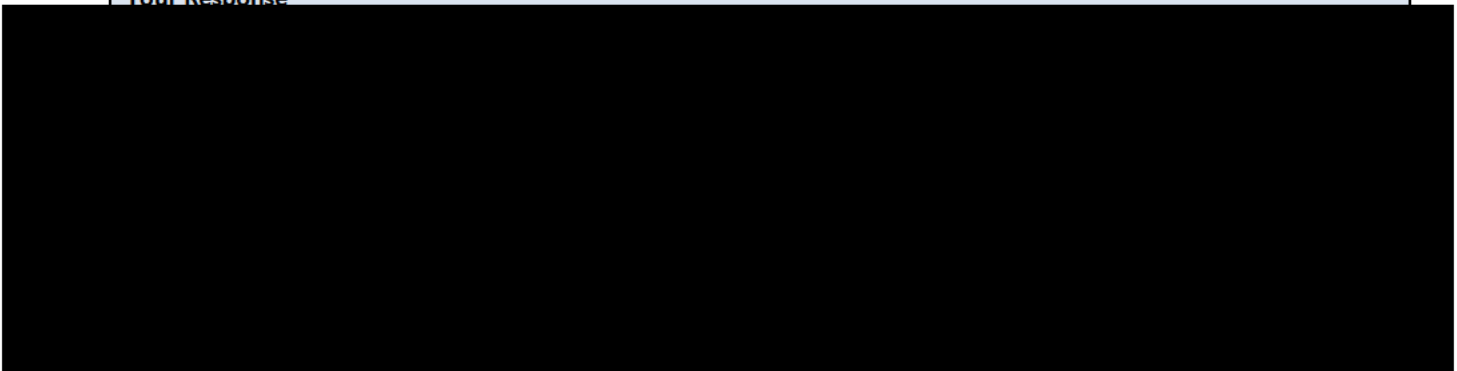
## STAGE 1: Compliance & Data Handling

1. General Compliance
2. Supplier Information
3. Form of Agreement
4. Certificate of Bona Fide Tendering
5. Information Security
6. Supplementary Terms and Conditions of Contract
7. Confidentiality and Security Requirements
8. Confidentiality Undertaking
9. Conflicts of Interest
10. Data Handling Assessment

Certificate of Bona Fide Tendering	
1.	I declare that this is a bona fide Tender, intended to be competitive and that I have not fixed or adjusted the amount of the Tender by or under or in accordance with any agreement or arrangement with any other person ('person' includes any persons any body or association, corporate or incorporate) except as disclosed on this Certificate under 7 below.
2.	I declare that the Company is not aware of any connection with a member of the Authority's staff which could affect the outcome of the bidding process.
3.	I declare that I have not done and I undertake that I shall not do at any time any of the following: <ol style="list-style-type: none"> <li>a) communicate to any person, including the addressee calling for the Tender, the amount or approximate amount of the proposed Tender;</li> <li>b) enter into any agreement or arrangement with any other person or body that he or it shall refrain from tendering or as to the amount of any Tender to be submitted;</li> <li>c) enter into any agreement or arrangement with any other person or body that we shall refrain from tendering on a future occasion;</li> <li>d) offer or pay or agree to pay any sum of money or valuable consideration directly or indirectly to any person for doing or causing to be done in relation to any other tender for the Services any act of the kind described above;</li> <li>e) canvas or solicit the Authority's staff.</li> </ol>
4.	I understand that any instances of illegal cartels or market sharing arrangements suspected by the Authority shall be referred to the Competition and Markets Authority for investigation and may be subject to action under the Competition Act 1998.
5.	I understand that any misrepresentations may also be the subject of criminal investigation or used as a basis for civil action.
6.	In this Certificate "agreement" or "arrangement" includes any transaction private or open, or collusion, formal or informal, and whether or not legally binding.
<b>Minimum Pass Mark:</b>	Completion
<b>Fail</b>	Information supplied is missing, incomplete or unqualified
<b>Pass</b>	Information supplied is complete and qualified



Your Response



## STAGE 1: Compliance & Data Handling

1. General Compliance
2. Supplier Information
3. Form of Agreement
4. Certificate of Bona Fide Tendering
5. **Information Security**
6. Supplementary Terms and Conditions of Contract
7. Confidentiality and Security Requirements
8. Confidentiality Undertaking
9. Conflicts of Interest
10. Data Handling Assessment

### Information Security Terms and Conditions

#### **Security Conditions:**

#### **Guidance for UK Contractors on the Protection of UK Assets marked as OFFICIAL - Sensitive**

1. The term "Authority" means the Contracting Authority.

#### **Security Grading**

2. The Authority shall issue a Security Aspects Letter which shall define the OFFICIAL - SENSITIVE information that is furnished to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all OFFICIAL - SENSITIVE documents which it originates or copies during the Contract clearly with the OFFICIAL - SENSITIVE classification.

#### **Official Secrets Acts**

3. The Contractor's attention is drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular. The Contractor shall take all reasonable steps to make sure that all individuals employed on any work in connection with the Contract (including sub-contractors) have notice that these statutory provisions, or any others provided by the Authority, apply to them and shall continue so to apply after the completion or earlier termination of the Contract.

#### **Protection of OFFICIAL - SENSITIVE Information**

4. The Contractor shall protect OFFICIAL - SENSITIVE information provided to it or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.
5. OFFICIAL - SENSITIVE information shall be protected in a manner to avoid unauthorised access. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.
6. All OFFICIAL - SENSITIVE material including documents, media and other material shall be physically secured to prevent unauthorised access. When not in use OFFICIAL - SENSITIVE documents/material shall be stored under lock and key. As a minimum, when not in use, OFFICIAL - SENSITIVE material shall be stored in a lockable room, cabinets, drawers or safe and the keys/combinations are themselves to be subject to a level of physical security and control.
7. Disclosure of OFFICIAL - SENSITIVE information shall be strictly in accordance with the "need to know" principle. Except with the written consent of the Authority, the Contractor shall not disclose any of the classified aspects of the Contract detailed in the Security Aspects Letter other than to a person directly employed by the Contractor or sub-Contractor, or Service Provider.

8. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and shall be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 26.

#### **Access**

9. Access to OFFICIAL - SENSITIVE information shall be confined to those individuals who have a “need-to-know” and whose access is essential for the purpose of his or her duties.

10. The Contractor shall ensure that all individuals having access to OFFICIAL - SENSITIVE information have undergone basic recruitment checks. Contractors shall apply the requirements of HMG Baseline Personnel Security Standard (BPSS) for all individuals having access to OFFICIAL - SENSITIVE information. Further details and the full requirements of the BPSS can be found at the GOV.UK website at:

<https://www.gov.uk/government/publications/security-policy-framework>

#### **Hard Copy Distribution of Information**

11. OFFICIAL - SENSITIVE documents shall be distributed, both within and outside company premises, in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post or Commercial Couriers in a single envelope. The words OFFICIAL - SENSITIVE shall **not** appear on the envelope. The envelope should bear a stamp or details that clearly indicate the full address of the office from which it was sent.

Advice on the distribution of OFFICIAL - SENSITIVE documents abroad or any other general advice including the distribution of OFFICIAL - SENSITIVE hardware shall be sought from the Authority.

#### **Electronic Communication, Telephony and Facsimile Services**

12. OFFICIAL - SENSITIVE information shall normally be transmitted over the internet encrypted using a 256 AES encryption.

Exceptionally, in urgent cases, OFFICIAL - SENSITIVE information may be emailed unencrypted over the internet **only** where there is a strong business need to do so and only with the **prior** approval of the Authority.

13. OFFICIAL - SENSITIVE information shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the authority shall require. Such limitations, including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the material.

14. OFFICIAL - SENSITIVE information may be discussed on fixed and mobile types of telephone within the UK, but not with (or within) earshot of) unauthorised persons.

15. OFFICIAL - SENSITIVE information may be faxed to UK recipients.

#### **Use of Information Systems**

16. The detailed functions that must be provided by an IT system to satisfy the minimum requirements described below cannot be described here; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

17. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.

18. The following describes the minimum security requirements for processing and accessing OFFICIAL - SENSITIVE information on IT systems.

a. Access: Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of “least privilege” shall be applied to System Administrators. Users of the IT System (Administrators should not conduct „standard“ User functions using their privileged accounts.

b. Identification and Authentication (ID&A): All systems shall have the following functionality:

(1) Up-to-date lists of authorised users.

(2) Positive identification of all users at the start of each processing session.

c. Passwords: Passwords are part of most ID&A Security Measures. Passwords shall be „strong“ using an appropriate method to achieve this, for example, including numeric and “special” characters (if permitted by the system) as well as alphabetic characters.

d. Internal Access Control: All systems shall have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission: Unless the Authority authorises otherwise, OFFICIAL - SENSITIVE information shall be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using a Foundation Grade product or equivalent as described in paragraph 12 above.

f. Security Accounting and Audit: Security relevant events fall into two categories, namely legitimate events and violations.

(1) The following events shall always be recorded:

- I. All log on attempts, whether successful or failed.
- II. Log off (including time out where applicable).
- III. The creation, deletion or alteration of access rights and privileges.
- IV. The creation, deletion or alteration of passwords.

(2) For each of the events listed above, the following information is to be recorded:

- V. Type of event
- VI. User ID
- VII. Date & Time
- VIII. Device ID

The accounting records shall have a facility to provide the System Manager with a hard copy of all or selected activity. There shall also be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know.

If the operating system is unable to provide this then the equipment shall be protected by physical means when not in use, i.e. locked away or the hard drive removed and locked away.

g. Integrity & Availability: The following supporting measures shall be implemented:

- 1. Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations)
- 2. Defined Business Contingency Plan
- 3. Data backup with local storage
- 4. Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software).
- 5. Operating systems, applications and firmware should be supported
- 6. Patching of Operating Systems and Applications used shall be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk shall be documented.

h. Logon Banners: Wherever possible, a “Logon Banner” shall be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring.

i. suggested format for the text depending on national legal requirements could be: “Unauthorised access to this computer system may constitute a criminal offence”.

j. Unattended Terminals: Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

k. Internet Connections: Computer systems shall not be connected direct to the Internet or „untrusted“ systems unless protected by a firewall (a software based personal firewall is the minimum) which is acceptable to the Authority’s Principal Security Advisor.

l. Disposal: Before IT storage media (e.g. disks) are disposed of, an erasure product shall be used to overwrite the

data. This is a more thorough process than deletion of files, which does not remove the data.

### **Laptops**

19. Laptops holding any supplied or contractor generated OFFICIAL - SENSITIVE information are to be encrypted using a Foundation Grade product of equivalent as described in paragraph 12 above.

20. Unencrypted laptops not on a secure site<sup>2</sup> are to be recalled and only used or stored in an appropriately secure location until further notice or until approved full encryption is installed. Where the encryption policy cannot be met, a Risk Balance Case that fully explains why the policy cannot be complied with, and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the Authority for consideration. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites. For the avoidance of doubt, the term “drives” includes all removable, recordable media (e.g. memory sticks, compact flash, recordable optical media (e.g. CDs and DVDs), floppy discs and external hard drives.

21. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

22. Portable CIS devices are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven, the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

<sup>2</sup> Secure Sites are defined as either Government premises or a secured office on the contractor premises

### **Loss and Incident Reporting**

23. The contractor shall immediately report any loss or otherwise compromise of OFFICIAL - SENSITIVE information to the Authority. Any security incident involving OFFICIAL - SENSITIVE information shall be immediately reported to the Authority.

### **Sub-Contracts**

24. The use of any sub-contractors must be stated in the Data Protection Impact Assessment (DPIA). If during the course of the contract it is decided to sub-contract work this must be reflected in an updated DPIA and this be approved by the Data Protection Officer of the CMA.

If the Sub-contract is approved, the Authority shall provide the Contractor with the security conditions that shall be incorporated within the Sub-contract document.

### **Publicity Material**

25. Contractors wishing to release any publicity material or display hardware that arises from this contract shall seek the prior approval of the Authority. Publicity material includes open publication in the contractor's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the Authority or any other government department.

### **Destruction**

26. As soon as no longer required, OFFICIAL - SENSITIVE information/material shall be destroyed in such a way as to make reconstitution unlikely, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when information/material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Contractor to be necessary or desirable. Unwanted OFFICIAL - SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

#### Interpretation/Guidance

27. Advice regarding the interpretation of the above requirements should be sought from the Authority.

#### Audit

28. Where considered necessary by the Authority, the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractors processes and facilities by representatives of the Authority to ensure compliance with these requirement.

#### SECURITY ASPECTS LETTER

1. The above work arises from a United Kingdom government contract and will involve your company holding UK classified material. It shall be a condition of the Contract that this material must be protected. The standard of protection required has been notified to you separately and varies with the level of classification. Material passed to you will bear the classification appropriate to it. However to assist you in allocating any necessary classification to material which your company may produce during the course of the Contract and thus enable you to provide the appropriate degree of protection to it, this letter formally advises you of the correct classification to apply to the various aspects of the Contract.

2. The aspects of the Contract which require to be classified are:

ASPECTS	CLASSIFICATION
Commercially sensitive information	Official sensitive
Internal communications within the CMA	Official / Official sensitive
External communications within the CMA and other stakeholders	Official / Official sensitive
Personal data	Official sensitive

3. If the Contract contains a Condition of Clause referring to "Secret Matter" this Secret matter is defined as the Aspects listed above.

4. You are requested to acknowledge receipt of this letter and to confirm that the level of classification associated with the various aspects listed above have been brought to the attention of the person directly responsible for the security of this Contract, that they are fully understood, and that the required security controls in the contract security conditions can and shall be taken to safeguard the material concerned.

5. If you have any difficulty in interpreting the meaning of the above aspects or in safeguarding the materials, please contact [REDACTED] immediately on the following:

[REDACTED]

Minimum Pass Mark:	Completion
Fail	Information supplied is missing, incomplete or unqualified
Pass	Information supplied is complete and qualified

Call-Off Schedule 20 (Call-Off Specification)

Call-Off Ref:

Crown Copyright 2018

on behalf of	
Company Name	Insight Direct (UK) Ltd

## STAGE 1: Compliance & Data Handling

1. General Compliance
2. Supplier Information
3. Form of Agreement
4. Certificate of Bona Fide Tendering
5. Information Security
6. **Supplementary Terms and Conditions of Contract**
7. Confidentiality and Security Requirements
8. Confidentiality Undertaking
9. Conflicts of Interest
10. Data Handling Assessment

### Supplementary Terms and Conditions of Contract

1. Authorised Representative
  - 1.1. The below person (including any successor in office from time to time of such person) is authorised to act as the CMA's Representative on all matters concerning this Contract:
  - 1.2. Each of the CMA and the Contractor may from time to time by notice in writing to the other party appoint another person to act as its authorised representative. Both parties shall use their reasonable endeavours to ensure that any such substitutions and or additions do not have any adverse impact on the Services.
2. Indemnities and Insurance
  - 2.1. The Contractor shall hold harmless and indemnify the CMA on demand from and against all claims, demands, proceedings, actions, damages, costs (including legal costs), expenses and any other liabilities arising from claims made by the CMA's staff or agents, or by third parties, in respect of any death or personal injury, or loss or destruction of or damage to property, or any other loss, destruction or damage, including but not limited to financial losses which are caused, whether directly or indirectly, by the breach of contract or breach of duty (whether in negligence, tort, statute or otherwise) of the Contractor, its employees, agents or sub-contractors.
  - 2.2. The Contractor shall be liable to the CMA for any loss, damage, destruction, injury or expense, whether direct or indirect, (and including but not limited to loss or destruction of or damage to the CMA's property, which includes data) arising from the Contractor's breach of contract or duty (whether arising in negligence, tort, statute or otherwise).
  - 2.3. Nothing in these Conditions or in any part of the Contract shall impose any liability on any member of the staff of the CMA or its representatives in their personal capacity.
  - 2.4. The Contractor shall indemnify the CMA against all proceedings, actions, claims, demands, costs (including legal costs), charges, expenses and any other liabilities arising from or incurred by reason of any infringement or alleged infringement of any third party's Intellectual Property Rights used by or on behalf of the Contractor for the purpose of the Contract, providing that any such infringement or alleged infringement is not knowingly caused by, or contributed to, by any act of the CMA.
  - 2.5. The CMA shall indemnify the Contractor against all proceedings, actions, claims, demands, costs (including legal costs), charges, expenses and any other liabilities arising from or incurred by reason of any infringement or alleged infringement of any third party's Intellectual Property Rights used at the request of the CMA by the Contractor in the course of providing the Services, providing that any such infringement or alleged infringement is not knowingly caused by, or contributed to by, any act of the Contractor.
  - 2.6. Except in relation to death or personal injury as referred to in Condition 2.1 and subject to Conditions 2.4 and 2.5 the amount of liability under this Condition shall be limited to the amounts stated in section 11.1 and 11.2 of the RM6098 Core Terms.
  - 2.7. The CMA shall not be liable under to pay any sum which:
    - 2.7..1. was claimable under insurance held by the Contractor, and the Contractor has failed to make a claim on its insurance, or has failed to make a claim in accordance with the procedural requirements of the insurance policy;
    - 2.7..2. when added to any sums paid or due to the Contractor under the Contract exceeds the total sum that



would have been payable to the Contractor if the Contract had not been terminated prior to the expiry of the Contract Duration; or

- 2.7...3. is a claim by the Contractor for loss of profit or any indirect or consequential loss, due to early termination of the Contract.

3. Conflicts of Interest

- 3.1. The Contractor shall disclose to the CMA's Representative as soon as is reasonably practical after becoming aware of any actual or potential conflict of interest relating to provision of the Services by the Contractor or any event or matter (including without limitation its reputation and standing) of which it is aware or anticipates may justify the CMA taking action to protect its interests.

4. Survival of the Contract

- 4.1. Insofar as any of the rights and obligations of the parties in this Contract shall or may be exercised after expiry or termination of the Contract, the provisions of the Contract conferring such rights and powers shall survive and remain in full force and effect notwithstanding such termination or expiry or any other contract with the CMA.

5. Working Time Directive

- 5.1. The Contractor shall ensure that the Working Time Directive Employment Regulations shall be applied in the proper manner to all personnel supplied via this Contract.
- 5.2. The Contractor shall ensure that commensurate with good employment practices and policies observed by the CMA, that all employment legislation is applied appropriately to all workers employed in providing the Services.

6. Observance of Statutory Requirements

- 6.1. The Contractor insofar as it is legally liable shall comply with all statutory requirements to be observed and performed in connection with the Contract and shall indemnify the CMA against all actions, claims, demands, proceedings, damages, costs, charges and expenses whatsoever in respect of any breach of statutory obligations.

7. Equal Opportunities and Harassment

- 7.1. The Contractor shall adopt a policy to comply with the requirements of the Race Relations Act 1976, the Race Relations (Amendment) Act 2000, the Employment Equality (Religion or Belief) Regulations 2003, the Sex Discrimination Act 1975 as amended, Equal Pay Act 1970, Employment Equality (Sexual Orientation) Regulations 2003, Sex Discrimination (Gender Reassignment) Regulations 1999, and the Disability Discrimination Act 1995 and the Disability Discrimination Act 2005, and accordingly, shall not treat one individual or group of people less favourably than others because of colour, race, nationality, ethnic origin, religion, gender, sexual orientation or disability and, further, shall seek to promote equality among its workers and generally. The Contractor shall note the CMA's current and future obligations under these Acts and under the Data Protection Act 2018, Freedom of Information Act 2000, Human Rights Act 1998, and any codes of practice and best practice guidance issued by the Government and the appropriate enforcement agencies.
- 7.2. The Contractor shall comply with the above legislation in so far as it places obligations upon the Contractor in the performance of its obligations under this Contract. The Contractor shall facilitate the CMA's compliance with the CMA's obligations under these provisions and comply with any request from the CMA for that purpose.
- 7.3. In the event of any finding of unlawful racial, disability or sexual discrimination being made against the Contractor by any court or industrial tribunal, or of an adverse finding in any formal investigation by the Equality and Human Rights Commission the Contractor shall take appropriate steps to prevent repetition of the unlawful discrimination and shall on request provide the CMA with details of any steps taken.
- 7.4. The Contractor shall set out its policies on race relations, sex discrimination and disability discrimination:
- in instructions to those concerned with recruitment, training and promotion;
  - in documents available to its personnel, recognised trade unions or other representative groups of its personnel; and

- in recruitment advertisements and other literature.

- 7.5. The Contractor shall, on request provide the CMA with copies of its policies, examples of the instructions and other documents, recruitment advertisements and other literature.
- 7.6. The Contractor shall provide such information as the CMA may reasonably request for the purpose of assessing the Contractor's compliance with this Condition 7.
- 7.7. The Contractor shall take all reasonable steps to ensure that Contractor's personnel engaged in the performance of the Contract do not act towards either CMA staff or members of the public in a manner that could amount to harassment on any of the grounds mentioned in 7.1. In the event of any finding of unlawful discrimination being made against the Contractor by any court or tribunal, or of any adverse finding in any formal investigation, the Contractor shall take appropriate steps to prevent repetition of the unlawful discrimination and shall, on request, provide the CMA with details of any steps taken.

#### 8. Payment

- 8.1. All invoices must be sent, quoting a valid purchase order number, to: The Competition and Markets Authority, Finance Team, The Cabot, 25 Cabot Square, London E14 4QZ. Within [10] working days of receipt of your countersigned copy of this letter, we will send you a Purchase Order (PO) with unique PO number. You must be in receipt of a valid PO number before submitting an invoice.
- 8.2. To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO number, PO number item number (if applicable) and the details (name and telephone number) of your customer contact (i.e. Contract Manager). Non-compliant invoices will be sent back to you, which may lead to a delay in payment. If you have a query regarding an outstanding payment please contact our Accounts Payable section either by email to [REDACTED] between 09:00-17:00 Monday to Friday.

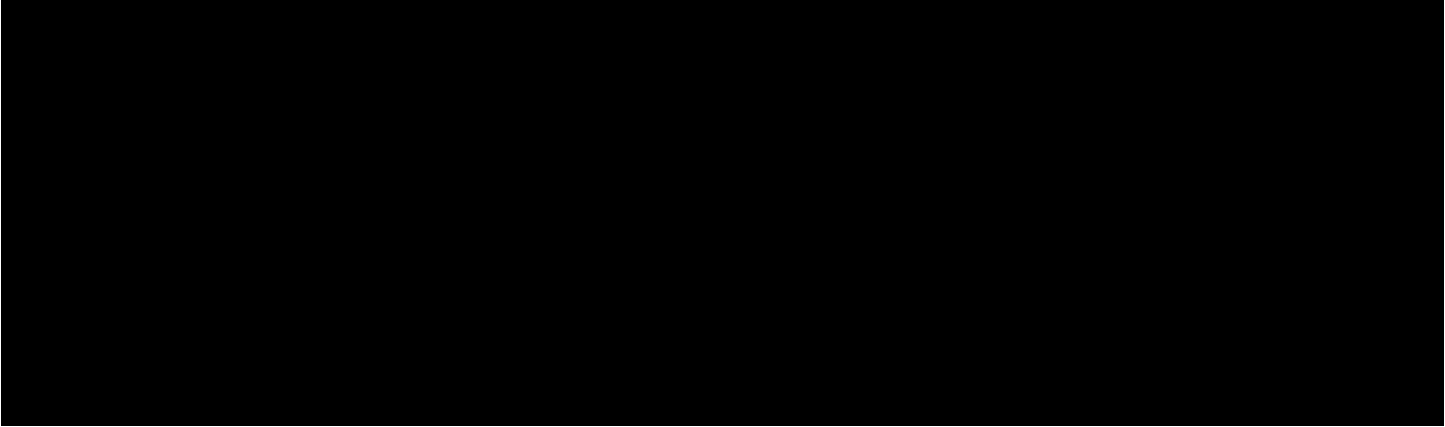
#### 9. Relevant Conviction

- 9.1. The CMA may require the Contractor to ensure that any person employed in the provision of Services has undertaken a Disclosure and Barring Service check. The Contractor shall ensure that no person who discloses that he/she has a conviction that is relevant to the nature of any Services, relevant to the work of the CMA, or is of a type otherwise advised by the CMA (each such conviction a "Relevant Conviction"), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a Disclosure and Barring Service check or otherwise) is employed or engaged in the provision of any part of the Services.

#### 10. Publicity

- 10.1. The service provider agrees not to disclose the identity of CMA as a client of the service provider, nor to use the CMA's name nor refer to the CMA directly or indirectly in any advertisement or other publication without receiving the CMA's prior written approval for such use or reference and to the form and context in which the reference to the CMA is to appear.
- 10.2. The service provider shall abide by any conditions or limitations imposed by the CMA in such approval, if given.
- 10.3. The service provider further agrees not to disclose the existence of this contract, or the nature of the relationship established by this contract.

#### CMA Representative



## STAGE 1: Compliance & Data Handling

1. General Compliance
2. Supplier Information
3. Form of Agreement
4. Certificate of Bona Fide Tendering
5. Information Security
6. Supplementary Terms and Conditions of Contract
7. Confidentiality and Security Requirements
8. Confidentiality Undertaking
9. Conflicts of Interest
10. Data Handling Assessment

### Confidentiality and Security Requirements

1. The secrecy and security aspects of the Competition & Markets Authority's work are governed by section 5 of the Official Secrets Act 1989, section 101 of the Telecommunications Act 1984, section 206 of the Water Industry Act 1991, section 74 of the Airports Act 1986, section 197 of the Broadcasting Act 1990, section 145 of the Railways Act 1993, Article 49 of the Airports (Northern Ireland) Order 1994, sections 348, 350(5) and 352 of the Financial Services and Markets Act 2000, Schedule 7 of the Postal Services Act 2000, section 105 of the Utilities Act 2000, Schedule 9 of the Transport Act 2000, section 245 of the Enterprise Act 2002, Article 63 of the Energy (Northern Ireland) Order 2003, section 393 of the Communications Act 2003 and Article 265 of The Water and Sewerage Services (Northern Ireland) Order 2006 (the Acts). Contractors shall be bound by the provisions of the Acts. Contractors should ensure that they fully understand the serious consequences that which may follow from a breach of any of these confidentiality requirements.
2. The confidentiality provisions of the Acts constitute a set of general restrictions on the disclosure of information obtained under the Acts in respect of particular businesses except when this is necessary for the purposes of the Act or for certain other prescribed purposes. Criminal prosecution is possible where unauthorised disclosure takes place. Most of the documents handled by the CMA fall within the scope of these statutory restrictions on disclosure and as 'sensitive documents' require the protection of effective security control and of strict observance of security rules. Contractors shall be expected to follow the CMA's security rules and these shall be discussed fully with them prior to commencement of the service.
3. Part V of the Criminal Justice Act 1993 also applies to information obtained in the course of CMA inquiries. It is a criminal offence under that legislation for members of a Contractor's staff to deal, or to encourage others to deal, in securities about which they hold inside information (i.e. unpublished price sensitive information relating to particular securities), obtained by virtue of their work for the CMA, or to disclose such information otherwise than in the proper performance of their work.
4. Contractors shall be responsible for ensuring that all staff employed in connection with any aspect of the service do not divulge any information obtained in, or as a result of, their work for the Competition and Markets Authority, except in the course of duty. The requirement not to divulge information includes not divulging information to other members of the Contractors' staff. Contractors shall also be responsible for ensuring that members of their staff are aware of and abide by the confidentiality provisions of the Acts and sign a witnessed declaration of the form set out on the following page. This

requirement shall include all support staff who may be involved in system administration or other duties which require them to be given access to any part of the Competition and Markets Authority network. A copy of each of these signed declarations shall be sent to the Contract Manager.

<b>Minimum Mark:</b>	<b>Pass</b>	For Information only
----------------------	-------------	----------------------

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

Call-Off Ref:

Crown Copyright 2018

### STAGE 1: Compliance & Data Handling

1. General Compliance
2. Supplier Information
3. Form of Agreement
4. Certificate of Bona Fide Tendering
5. Information Security
6. Supplementary Terms and Conditions of Contract
7. Confidentiality and Security Requirements
8. **Confidentiality Undertaking**
9. Conflicts of Interest
10. Data Handling Assessment

#### CONFIDENTIALITY UNDERTAKING, THE COMPETITION AND MARKETS AUTHORITY

I understand that in any work for 'the CMA' which I perform I shall be in possession of information which is held in confidence and which must not be disclosed without lawful authority. I am aware that the legislation referred to below provides for criminal prosecution where unauthorised disclosure takes place, and that on conviction a person may be fined or imprisoned. I am also aware that, in law, I owe duties of confidentiality to the CMA.

I accept that I must not communicate, orally or in writing, any information gained by me as a result of my work for the CMA to any person other than a person to whom it is my duty to communicate it without the consent of the Chief Executive of the CMA (or an authorised member of his staff). In the case of information with respect to any particular trade or business, I accept that the consent of the person carrying on that trade or business is required also. I accept that articles of any description prepared for publication or discussion in any written form or for broadcasting are covered by these conditions.

I also acknowledge that Part 9 of the Enterprise Act 2002 and Part V of the Criminal Justice Act 1993 applies to me and that it is a criminal offence to deal, or to procure others to deal, in securities about which I hold unpublished price sensitive information when engaged in work for or on behalf of the CMA.

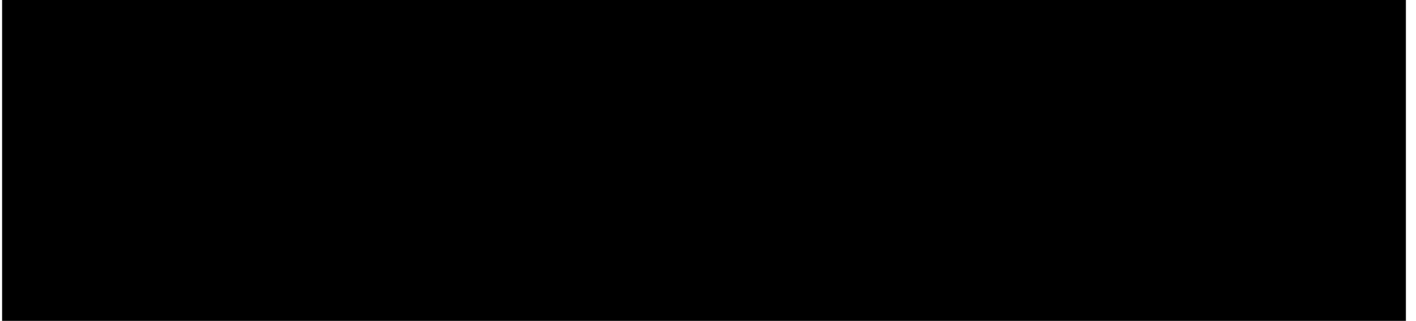
<b>Minimum Pass Mark:</b>	Completion
<b>Fail</b>	Information supplied is missing, incomplete or unqualified
<b>Pass</b>	Information supplied is complete and qualified
<b>Your response</b>	

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

Call-Off Ref:

Crown Copyright 2018

While the Contractor is working at the CMA's offices, the following people are to be contacted in case of an emergency:	
<b>Your response</b>	





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

Call-Off Ref:

Crown Copyright 2018

### STAGE 1: Compliance & Data Handling

1. General Compliance
2. Supplier Information
3. Form of Agreement
4. Certificate of Bona Fide Tendering
5. Information Security
6. Supplementary Terms and Conditions of Contract
7. Confidentiality and Security Requirements
8. Confidentiality Undertaking
9. Conflicts of Interest
10. Data Handling Assessment

### Conflicts of Interest in Relation to Contractors and Contractors' Staff

#### Summary

1. Contractors and their staff must disclose any interests which might give rise to a conflict or potential conflict to the CMA before entering into a contract with the CMA. The CMA will consider whether the potential conflict causes concern and what action (if any) should be taken. It may be necessary to require the disposal of an interest in order for the CMA to be able to enter into a contract.

#### Detail

2. When a Contractor is approached with a view to entering into a contract or call-off with the CMA, the Contractor must disclose to the CMA any potential conflict of interest of which it is aware, or becomes aware, affecting any of the following:
  - a) the Contractor, their spouse, or partner (other than a spouse) and dependents;
  - b) all personnel of the Contractor whose involvement on a contract with the CMA is not purely mechanical or clerical; and
  - c) all directors, partners and other senior personnel of a Contractor with equivalent responsibilities even though they are not involved in a contract with the CMA.
3. If the Contractor has any doubts as to whether or not there exists an interest which may give rise to a conflict, these doubts must also be disclosed.
4. In this annex the following terms have the meanings set out below:
  - a) "relevant individuals" means persons within sub-paragraphs 2 (a) to (c) above, together with their spouses, partners (other than a spouse) and dependents;
  - b) "the reference companies" means any company (incorporated or unincorporated), partnership, business or individual that is the subject of the reference relating to the Contract or Call-off to be awarded to the Contractor;
  - c) "the relevant companies" means any company (incorporated or unincorporated), partnership, business or individual who is a competitor, customer or supplier of any reference companies.
  - d) "shareholding" includes:
    - (i) shares, whether bearing a right to vote or not;
    - (ii) stock or debentures; and
    - (iii) options and similar rights;
    - (iv) in each case whatever the value of the holding and whether held as trustee or beneficially, (for example under a family trust or a Personal Equity Plan). Holdings in unit trusts, investment trusts, unit linked policies or similar arrangements under which the investor has interests in a large number of enterprises would not normally give rise to a potential conflict of interest, unless any company involved in the arrangements were itself affected by the inquiry. However, if the trust or arrangement specialises in investing in a particular industry which is affected by the reference or if the investor believes that there is a real possibility of the value of the investment being affected by the outcome of the reference, the interest should be disclosed to the CMA.



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

Call-Off Ref:

Crown Copyright 2018

5. The requirement under paragraph 3 to disclose any potential conflict of interest includes a requirement to disclose any relationship which may give an appearance of bias on the part of the Contractor or its staff including but not limited to:
  - a. the Contractor's present or past contractual relationship with any of the reference companies;
  - b. the Contractor's present or past contractual relationship with any of the relevant companies;
  - c. the Contractor's or relevant individuals' shareholding or partnership in, ownership (whether full or partial) or directorship of, or employment by:
    - (i) the reference companies;
    - (ii) the relevant companies; and
    - (iii) any enterprise the value of whose shares may be affected by the outcome of the reference (e.g. an enterprise in the same industry).
  - d. the Contractor's present or past contractual relationship with, or the Contractor's, or relevant individuals', employment by the relevant regulator (if applicable in relation to the reference);
  - e. the management of the investment of a shareholding or other interest of a person for which the Contractor, or any relevant individual, is responsible; and
  - f. a recent personal or family involvement with the reference companies or the relevant companies e.g. a substantial shareholding or other interest which has recently been disposed of.
6. Share accounts with a building society would not need to be disclosed except, for example, where they entitled the holder to a "perk" in the event of a merger. Similarly, bank accounts would not normally need to be disclosed in a reference involving the bank, though they should be disclosed where a person wishes to obtain or renegotiate a loan or overdraft.
7. A potential conflict of interest may arise in other circumstances, such as where there is a business relationship with an enterprise affected by the reference or any other close relationship with a person whose affairs may be affected by the reference. **In case of doubt the Contractor or relevant individual should disclose the interest.**
8. An interest as a consumer would not need to be disclosed, in normal circumstances, where the value of the goods or services obtained is small or most individuals are consumers (e.g. in the case of a market investigation into the supply of milk, salt or bread). If however the interest is that of a minority class of consumer there might be a conflict. This might be the case if, for example, an individual, his or her spouse, or child, were a coeliac and as such required gluten free products which were produced by companies involved in a merger reference.
9. The Contractor should check and relevant individuals as defined in paragraph 4 above should be required by the Contractor to check (if they are not already confident of the facts) their own shareholdings and shareholdings held on their behalf. They should also check, information which has been provided to them, e.g. as trustees or a holder of a specialised unit trust and whether they are aware in general terms of any conflict of interest.
10. The CMA will decide whether anything which has been disclosed as a potential conflict of interest constitutes an actual conflict in the particular circumstances. In some circumstances it may suffice for an interest which does give rise to a conflict to be disposed of in the period between public announcement of the reference and distribution of relevant papers, (subject to the approval of the CMA). In some circumstances it may be sufficient simply to inform the parties involved in the inquiry or likely to be involved of the interest (be it a shareholding or other interest).

## CONFLICTS OF INTEREST STATEMENT

### THE COMPETITION AND MARKETS AUTHORITY

1. We confirm that there is no conflict of interest that might give rise to a risk of challenge in the courts to the inquiry on the ground of bias (whether actual or apparent). The acceptance of the following terms and conditions shall be taken as confirmation that no such conflicts of interest exist.
2. We shall ensure that actual or even potential conflicts do not arise during the course of the inquiry. In particular:
  - a) For the duration of the inquiry we shall not undertake or actively seek any work for any organisation that is directly related to the subject of the inquiry. We agree that work which is indirectly related other than that laid out in the contract should only be undertaken with the CMA's consent which shall not be unreasonably withheld.
  - b) We confirm that any individuals providing services to the inquiry, as applicable, shall not carry out any work related to the subject of the inquiry for any other client for the duration of the inquiry. However, those individuals may consult colleagues who are engaged in such work in order to obtain information from them.

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

Call-Off Ref:

Crown Copyright 2018

- c) We confirm that individuals providing services to the inquiry and their immediate families do not own or have a beneficial interest in the shares of the main parties to the inquiry or their suppliers unless such holdings are independently managed (e.g. by a unit trust or pension fund).
- d) All information acquired by the individuals providing services to the inquiry shall be treated as confidential to the CMA both for the duration of the agreement and thereafter. The individuals shall not communicate it to third parties or other individuals within your firm unless it has already entered the public domain by other means. All documents supplied to us in connection with the inquiry and this agreement, copies of any part of such documents, whether in electronic or material form, and any documents prepared by us which are based on material supplied in connection with this inquiry, must be returned to the CMA at the end of the inquiry, or sooner if requested.
3. The CMA may terminate this contract at any time should it become of the opinion that an actual or potential conflict of interest on our part has arisen. We shall be entitled to remuneration on the basis set out in this letter up to the date of termination save in circumstances where we are in breach of our obligations under the terms of the contract.
4. It shall be our responsibility to ensure that no conflict of interest arises which might be said to prejudice our independence and objectivity in performing the contract. This responsibility includes all of our senior staff (e.g. directors, and partners) or our personnel whose involvement on the contract with the CMA is not purely mechanical or clerical. If we are at any time in doubt about whether any conflict of interest may exist or arise, we shall notify the CMA forthwith and comply with any directions given with a view to avoiding the conflict.
5. During the period of the contract, and for an **agreed period** after it ends, we would, **except with the prior written consent of the Contract Manager**, be debarred from working for, or having any other interest in, any of the main parties to the inquiry (which is the subject of the Contract) or any of their competitors in the relevant industry. This requirement is made to avoid conflicts of interest.
6. The acceptance of these terms and conditions shall be taken as confirming agreement on all of the above points.

Minimum Pass Mark:	Completion
Fail	Information supplied is missing, incomplete or unqualified
Pass	Information supplied is complete and qualified
Your Response	

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

Call-Off Ref:

Crown Copyright 2018

### STAGE 1: Compliance & Data Handling

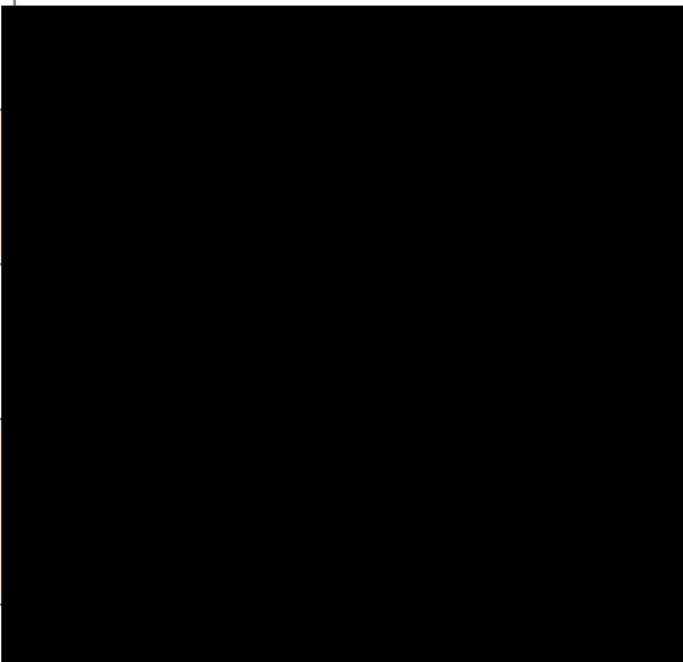
1. General Compliance
2. Supplier Information
3. Form of Agreement
4. Certificate of Bona Fide Tendering
5. Information Security
6. Supplementary Terms and Conditions of Contract
7. Confidentiality and Security Requirements
8. Confidentiality Undertaking
9. Conflicts of Interest
10. Data Handling Assessment

Data Handling Assessment	
Requirement:	CMA requires all Tenderers to complete the below Data Handling Assessment as part of their offer
	<b>Question Guidance</b>
	<b>Question 1:</b> In answering this question, Tenderers should:  Provide a response of 'No' to confirm Compliance with the CMA's requirement or 'Yes', to confirm non-compliance. If the Tenderer confirms a response of 'Yes', the tenderer is also required to advise which country.
	<b>Question 2:</b> In answering this question, tenderers should:  Provide a response of 'No' to confirm Compliance with the CMA's requirement or 'Yes', to confirm non-compliance. If the Tenderer confirms a response of 'Yes', the tenderer is also required to advise which country.
	<b>Question 3:</b> In answering this question, tenderers should:  If applicable, provide a response of 'Yes' and provided a draft IDTA and we agree to conclude this with the CMA or 'No', we have not provided a draft and shall not accept IDTA or N/A if the question doesn't apply.

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

Call-Off Ref:

Crown Copyright 2018

	<i>Tenderers who intend to process the CMA's data outside of the UK in performance of this contract, which cannot accept the relevant Standard Contractual Clauses (SCC) where still applicable or International Data Transfer Agreement, may fail.</i>	
	<b>Question 4:</b> In answering this question, tenderers should:  Provide details of any technical and organisational measures implemented.	
	<b>Question 5:</b> In answering this question, tenderers should:  Provide a list of any documented policies and processes your company has in place.	
	<b>Question 6:</b> In answering this question, tenderers should:  Provide all geographical locations which your company will be providing all or part of the contracted services to the CMA.	
<b>Minimum Pass Mark:</b>	<b>Completion</b>	
<b>Fail</b>	Information supplied is missing, incomplete or unqualified	
<b>Pass</b>	Information supplied is complete and qualified	
<b>YOUR RESPONSE</b>		
<b>No.</b>	<b>Question/Requirement</b>	<b>Response</b>
1.	Please confirm whether your company will process/transfer any of the Authority data outside of the UK.	
1.a	<i>In case of question 1 above your response is "Yes", in which countries will your company process/transfer the Authority's data?</i>	
2.	Please confirm whether your company's sub contractors/sub processors will process/transfer any of the Authority data outside the UK	
2.a	<i>In case of question 2 above your response is "Yes", in which countries will your sub-contrators/processors process/transfer the Authority's data?</i>	
3	If you have advised of a country outside of the United Kingdom,	

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

Call-Off Ref:

Crown Copyright 2018

	you will be required to provide a draft of the International Data Transfer Agreement (IDTA) as issued by ICO, and to conclude this agreement with the CMA.	
4	Provide full details of any technical and organisational measures implemented to protect Personal Data in compliance with the data security requirements of the data protection legislation.	
5	List any documented policies and processes your company has in place to support their data protection obligations e.g. Breach Management & Notification, Data Subject Rights etc.	
6	Clearly specify all geographical locations from which your company will be providing all or part of the contracted services to the CMA. This includes any cloud based hosting, third party SaaS services, customer support services, third party	

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

Call-Off Ref:

Crown Copyright 2018

	contractors or agencies processing on behalf of the Tenderers and geographical location of permanent and/or temporary staff involved in providing services to the CMA.	
--	--	--

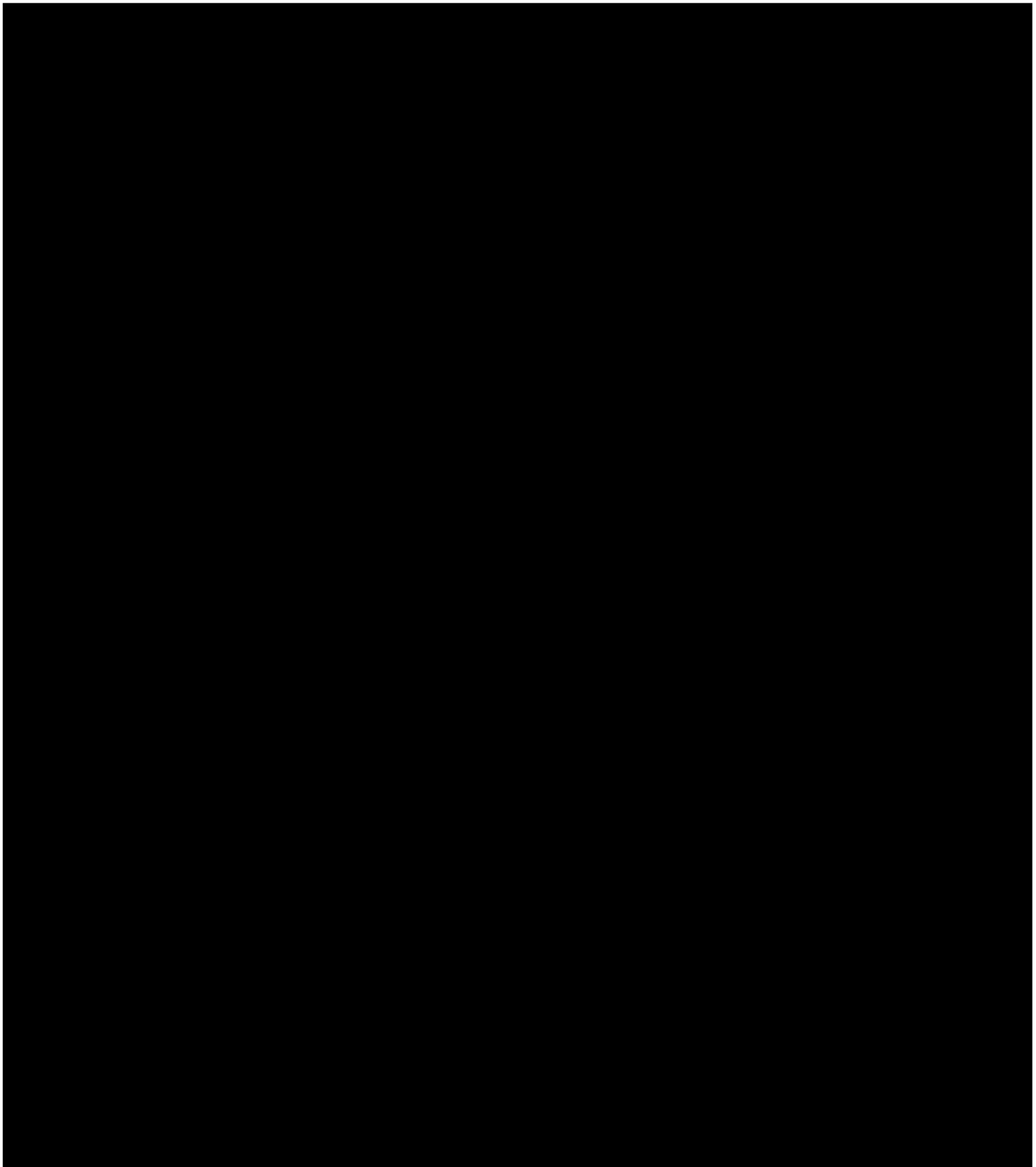
## Annex 2 – Quality Response Document (Insight’s Response to Annex 4 of the ITT)

Contract Reference: Provision of a Cisco Partner

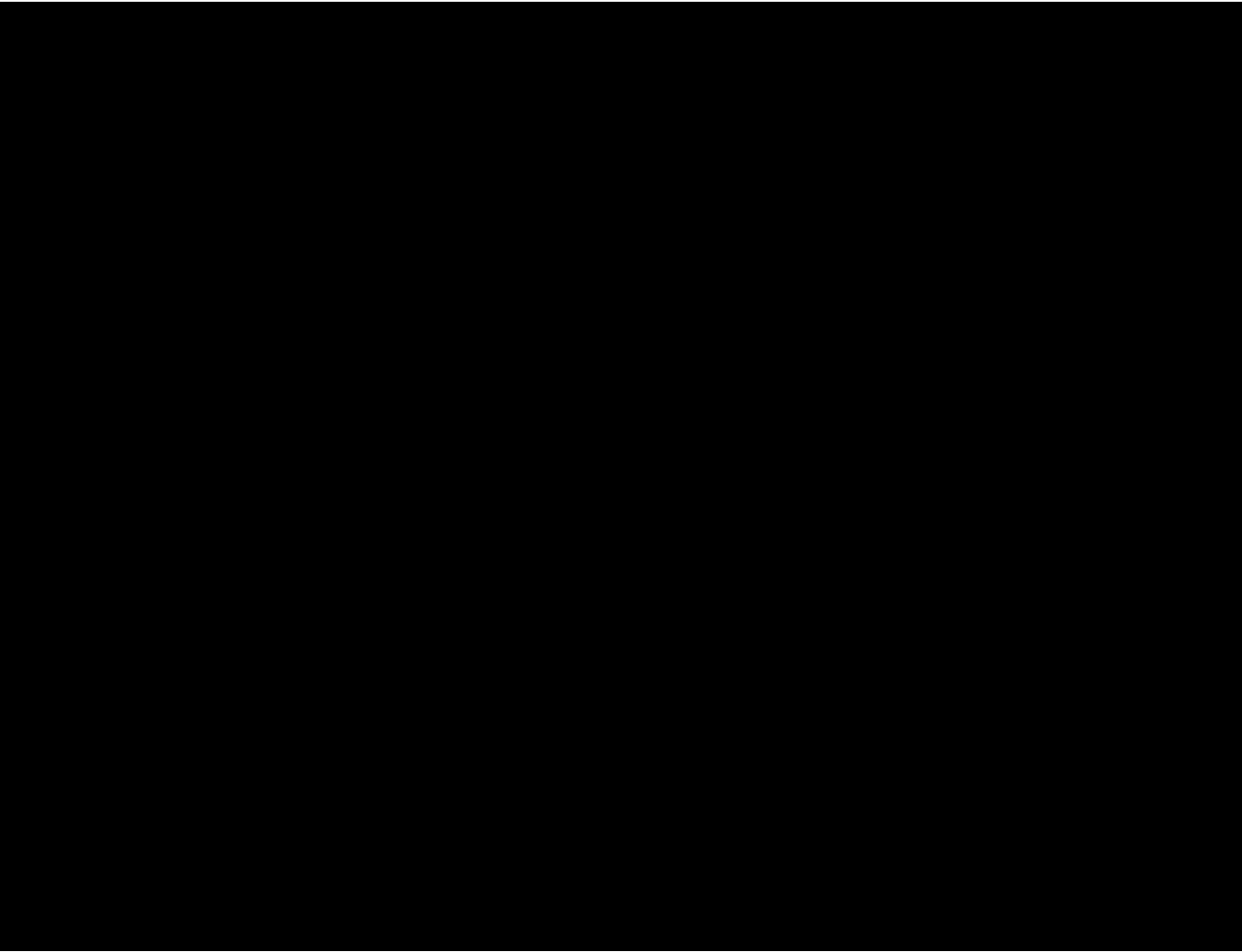
Procurement Reference: **PROC-884-2024**

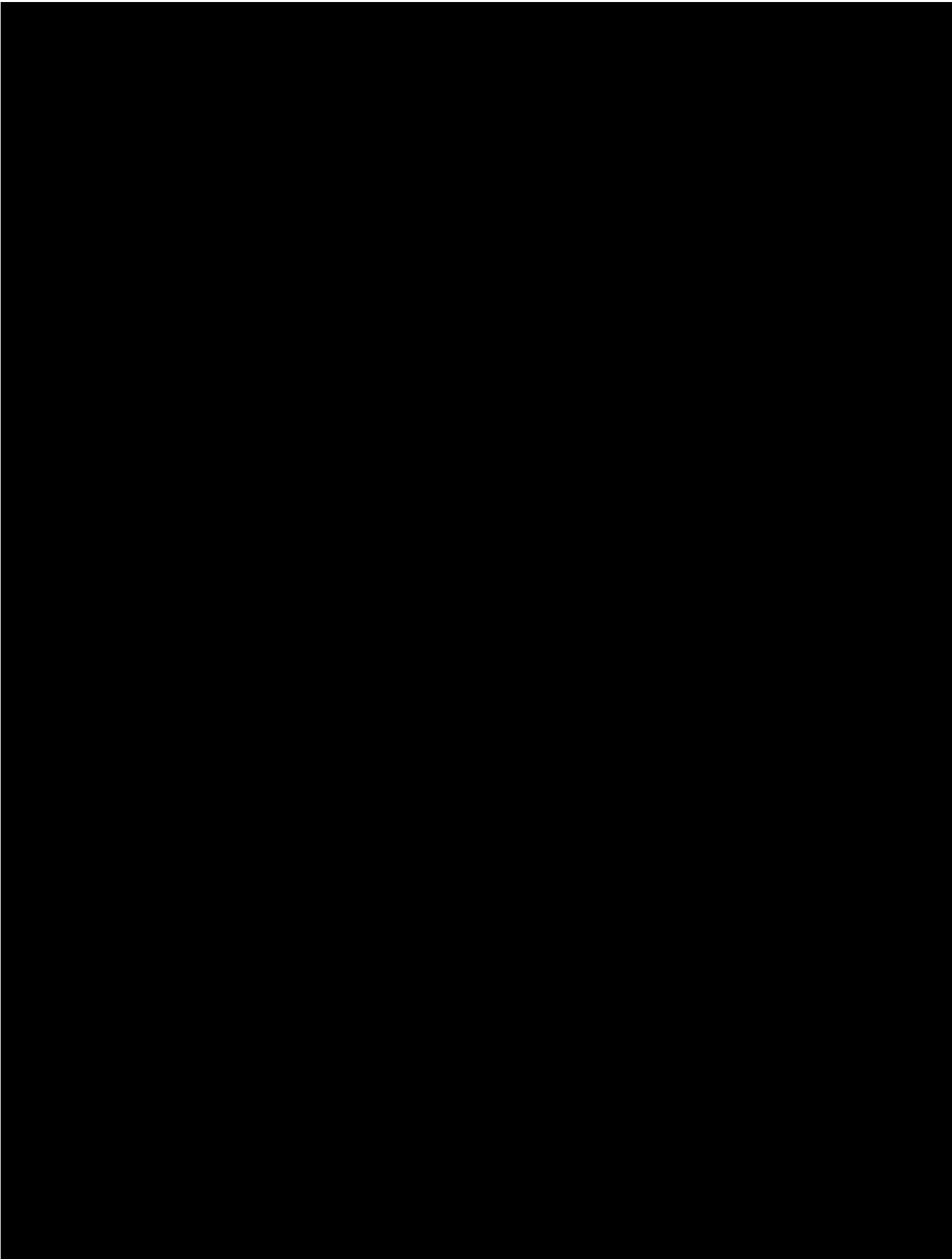


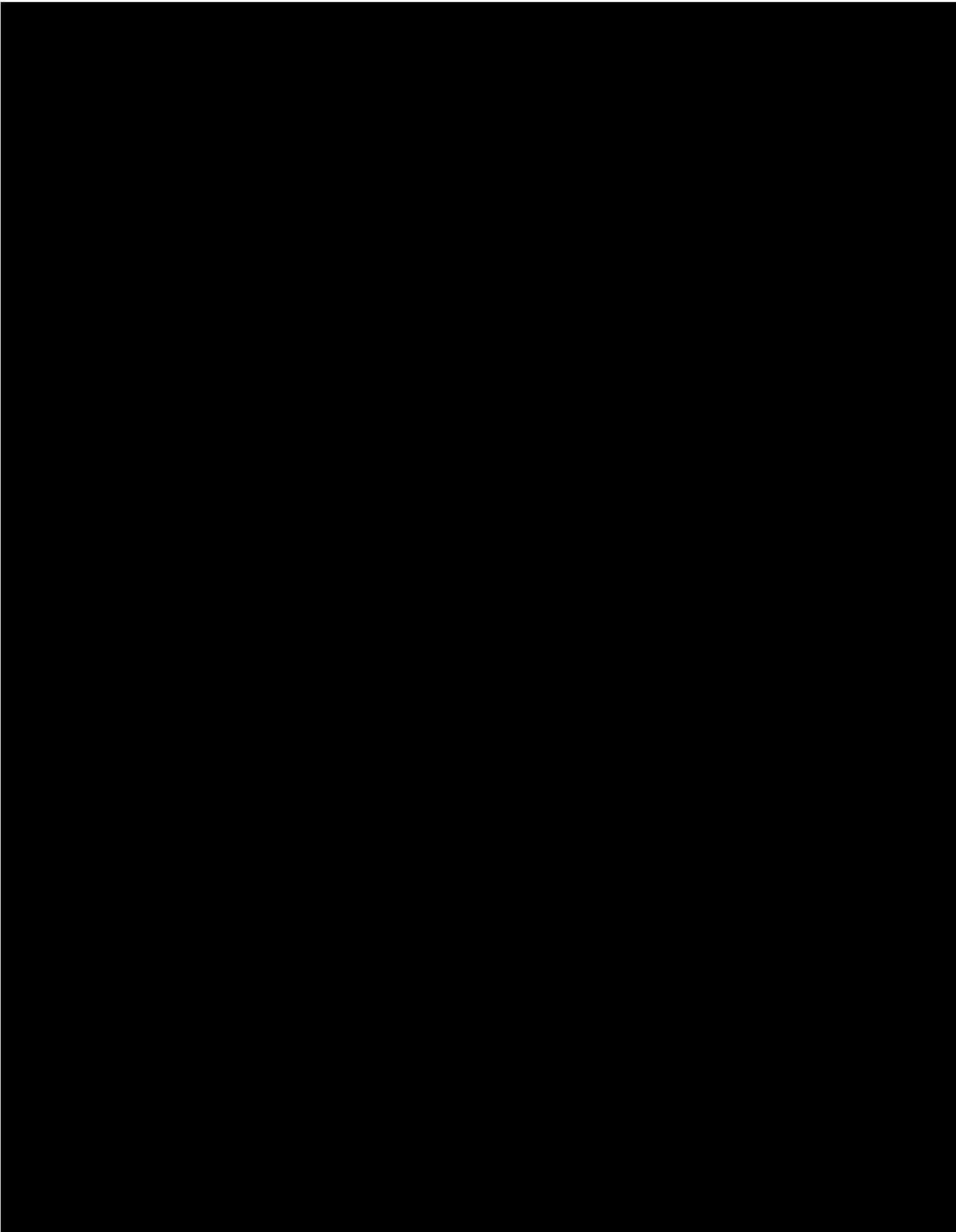
SCORED QUESTIONS	
1 - Vulnerabilities	
<p>Over the term of the contract, Cisco software vulnerabilities may arise. Please advise on the types of vulnerabilities you assess against, how you provide notification and how you would keep this list up to date.</p>	
<p><b><u>Response Guidance:</u></b></p> <p>Responses must be provided in aerial font, size 11 and are limited to a maximum of 1000 words, excluding pictures, tables and organograms (if required).</p>	
Score Available	10%
<i>'Please enter your response here'</i>	

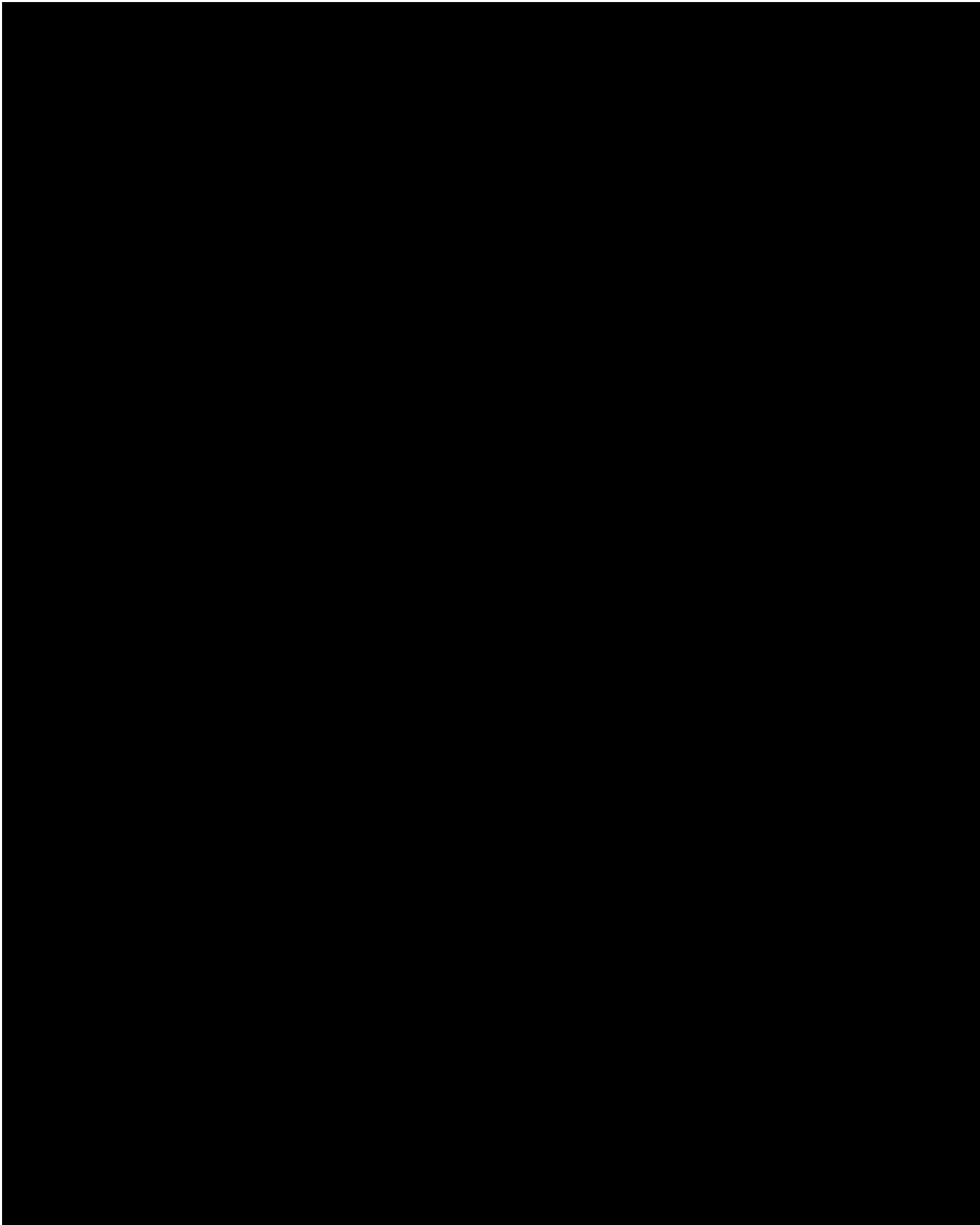












Please detail your relevant experience as a Cisco reseller and how you would apply this experience to the CMA's Cisco Partner contract.

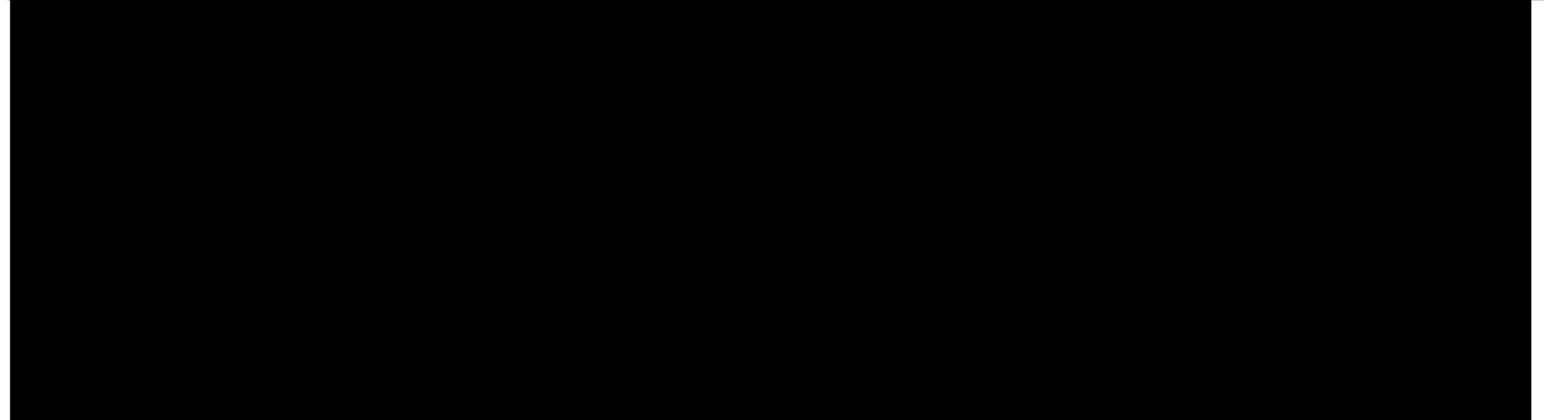
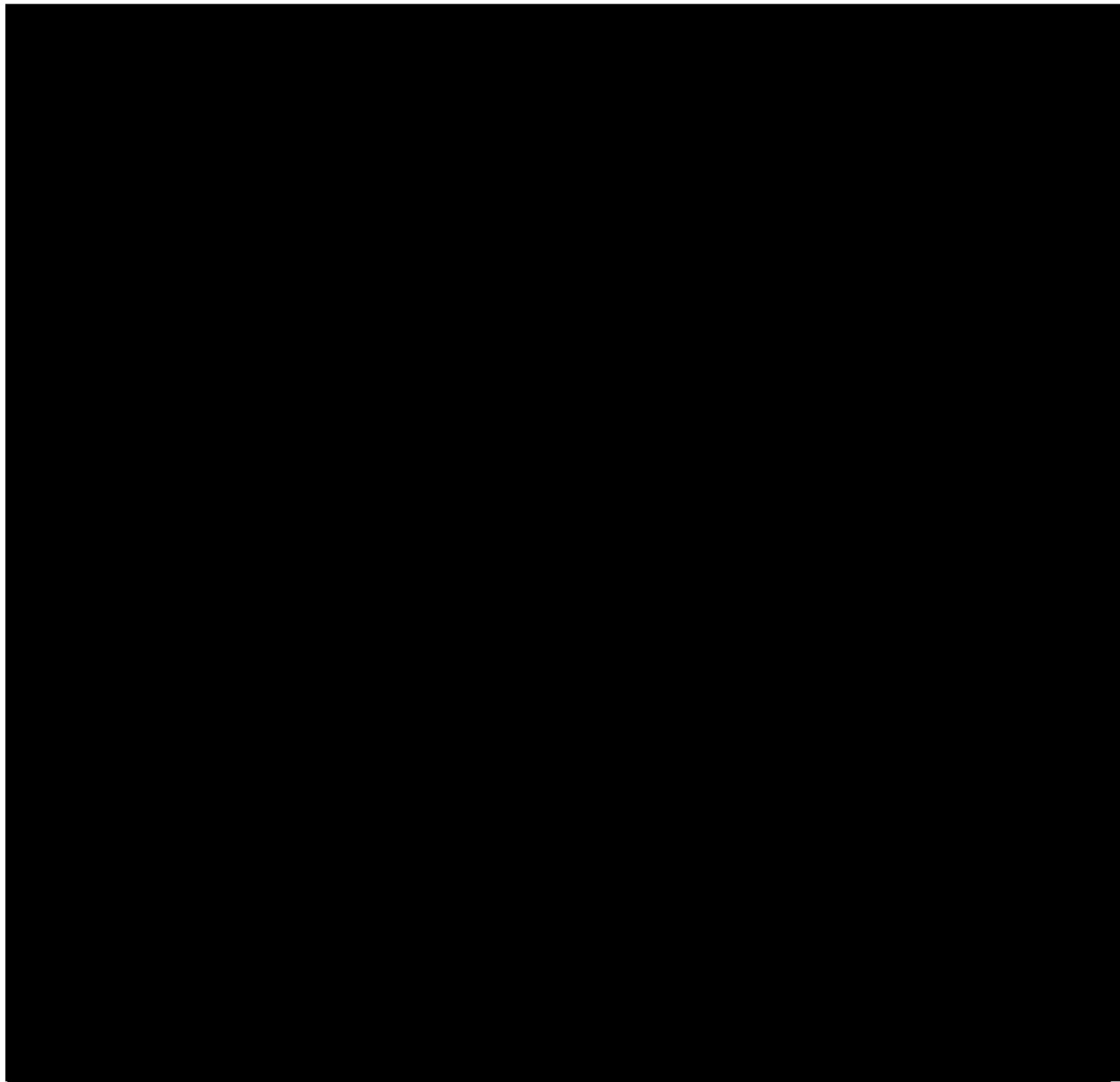
**Response Guidance**

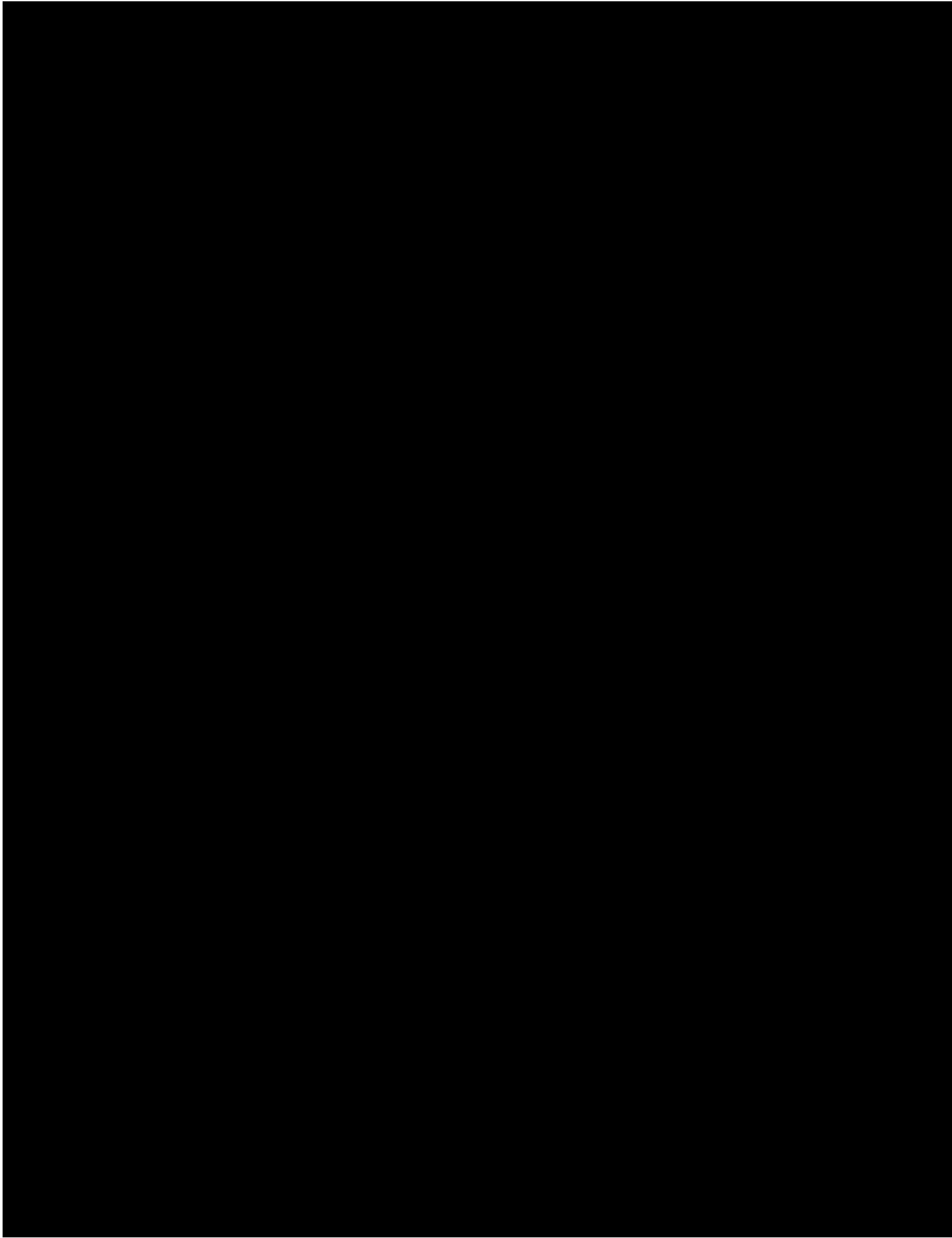
Responses must be provided in aerial font, size 11 and are limited to a maximum of 1000 words, excluding pictures, tables and organograms (if required).

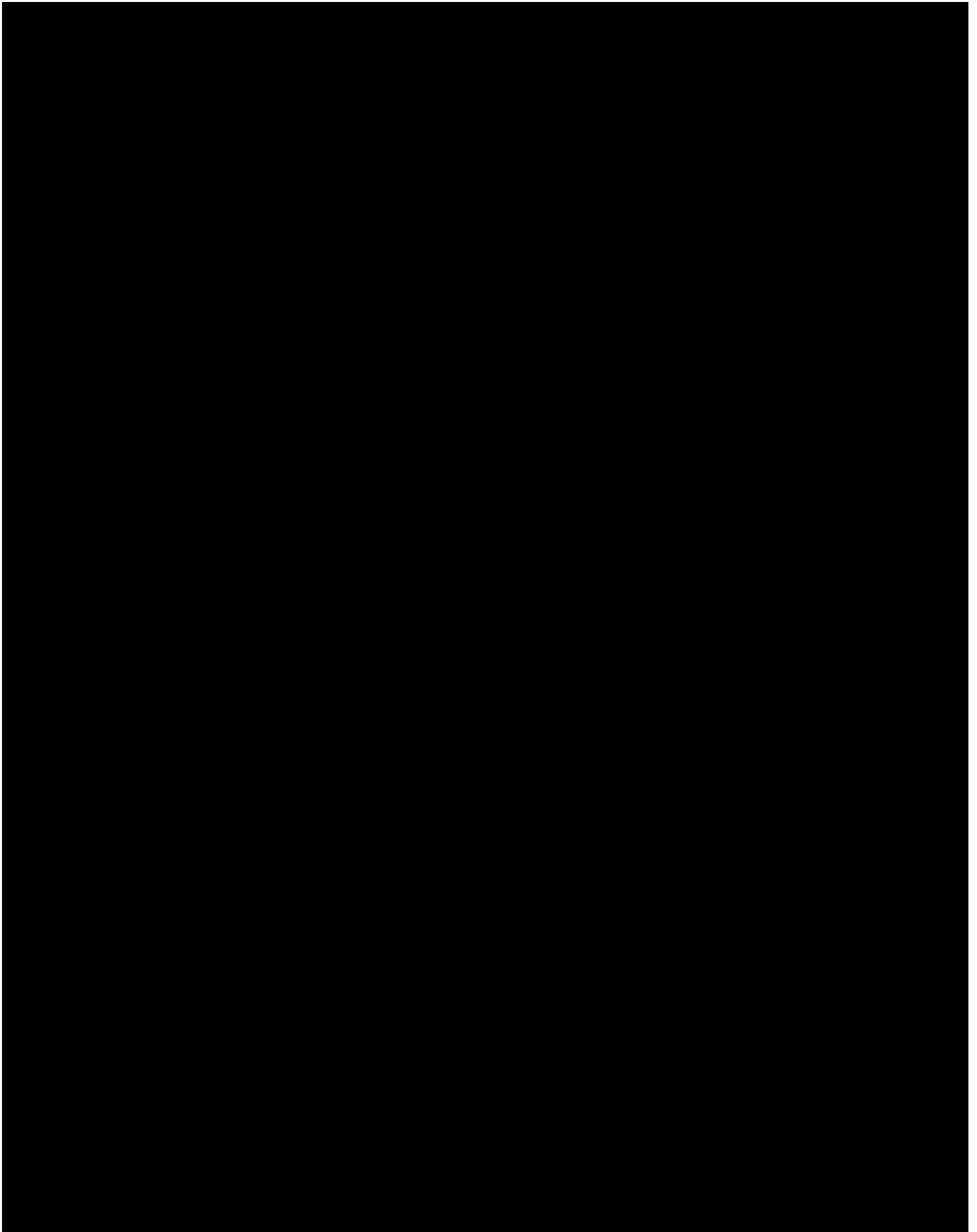
**Score Available**

**45%**

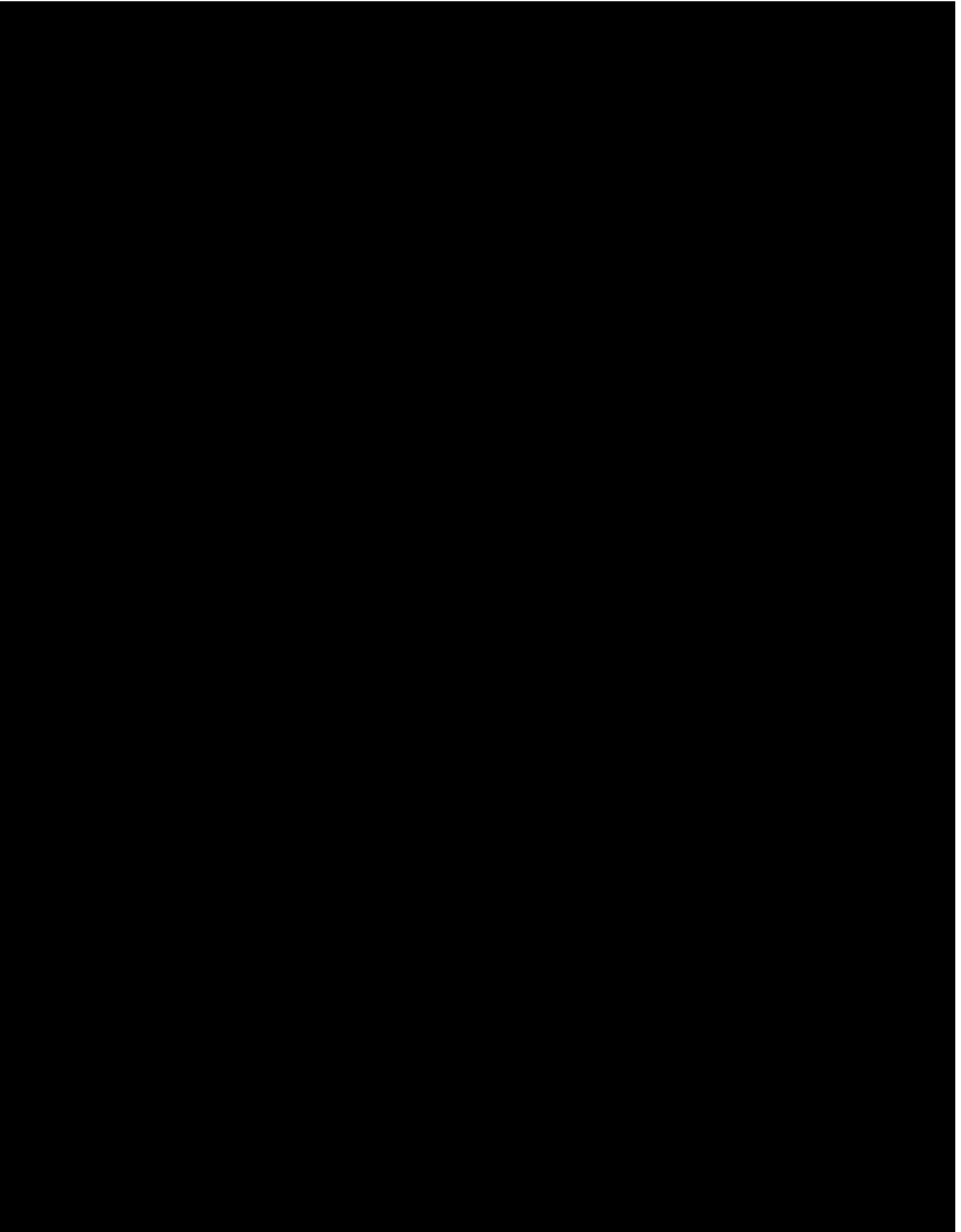
*'Please enter your response here'*

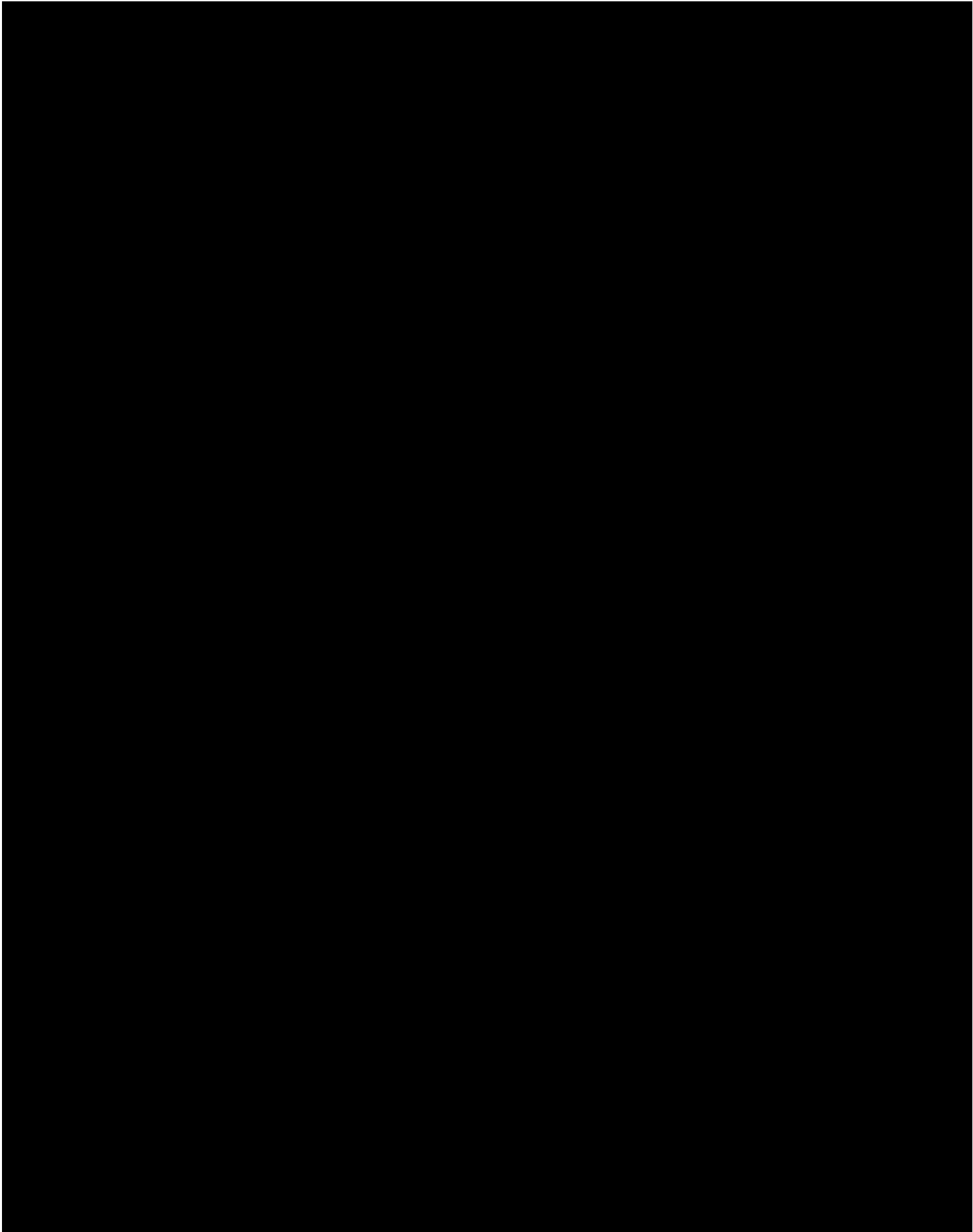














Word Count	<i>Word Count: 938</i>
------------	------------------------

### 3 – Account Management

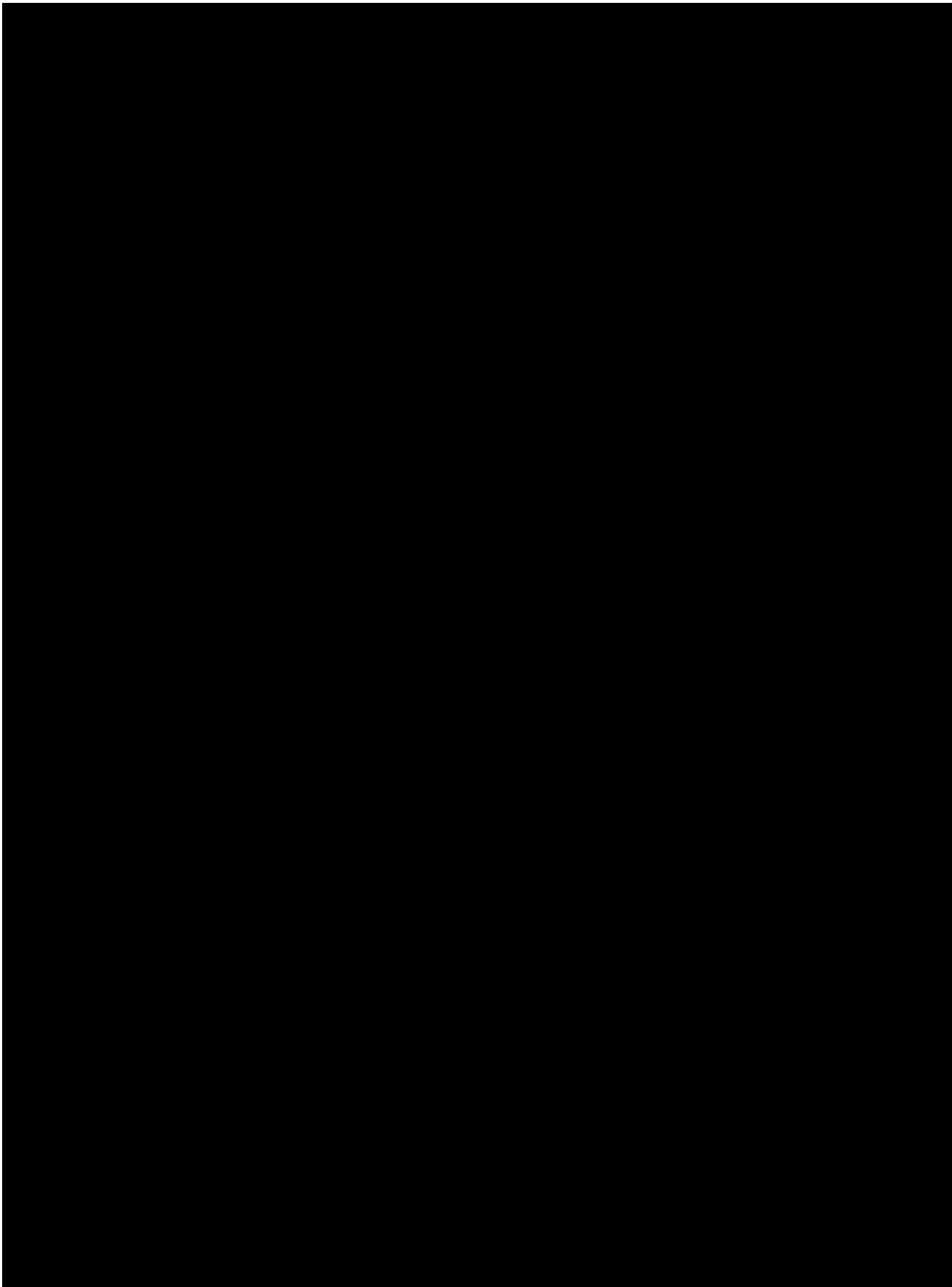
Please provide details of how you will manage the account and how you will work with the CMA project portfolio team, noting project timescales could change.

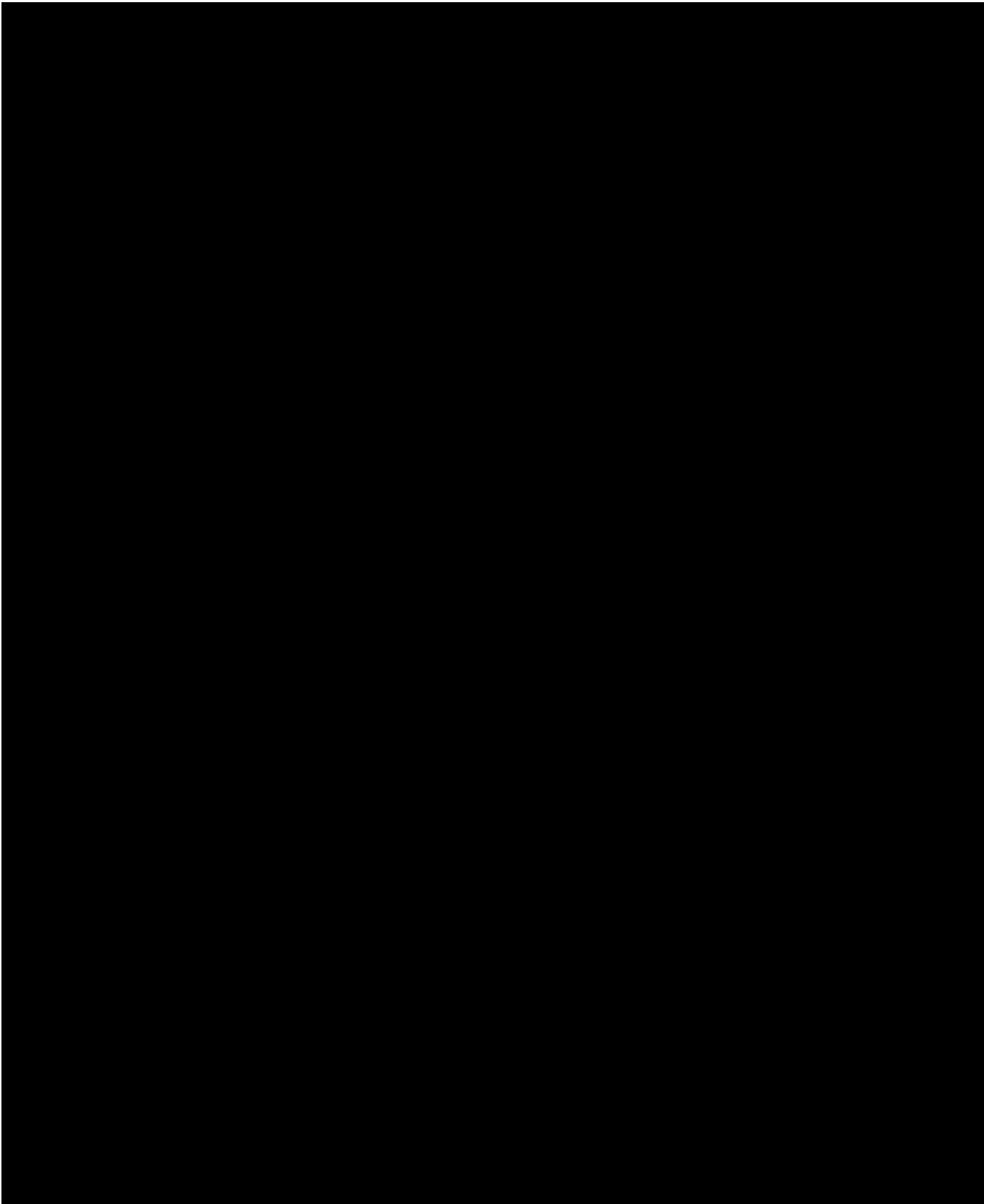
#### **Response Guidance**

Responses must be provided in aerial font, size 11 and are limited to a maximum of 1000 words, CV's are excluded, excluding pictures, tables and organograms (if required).

Score Available

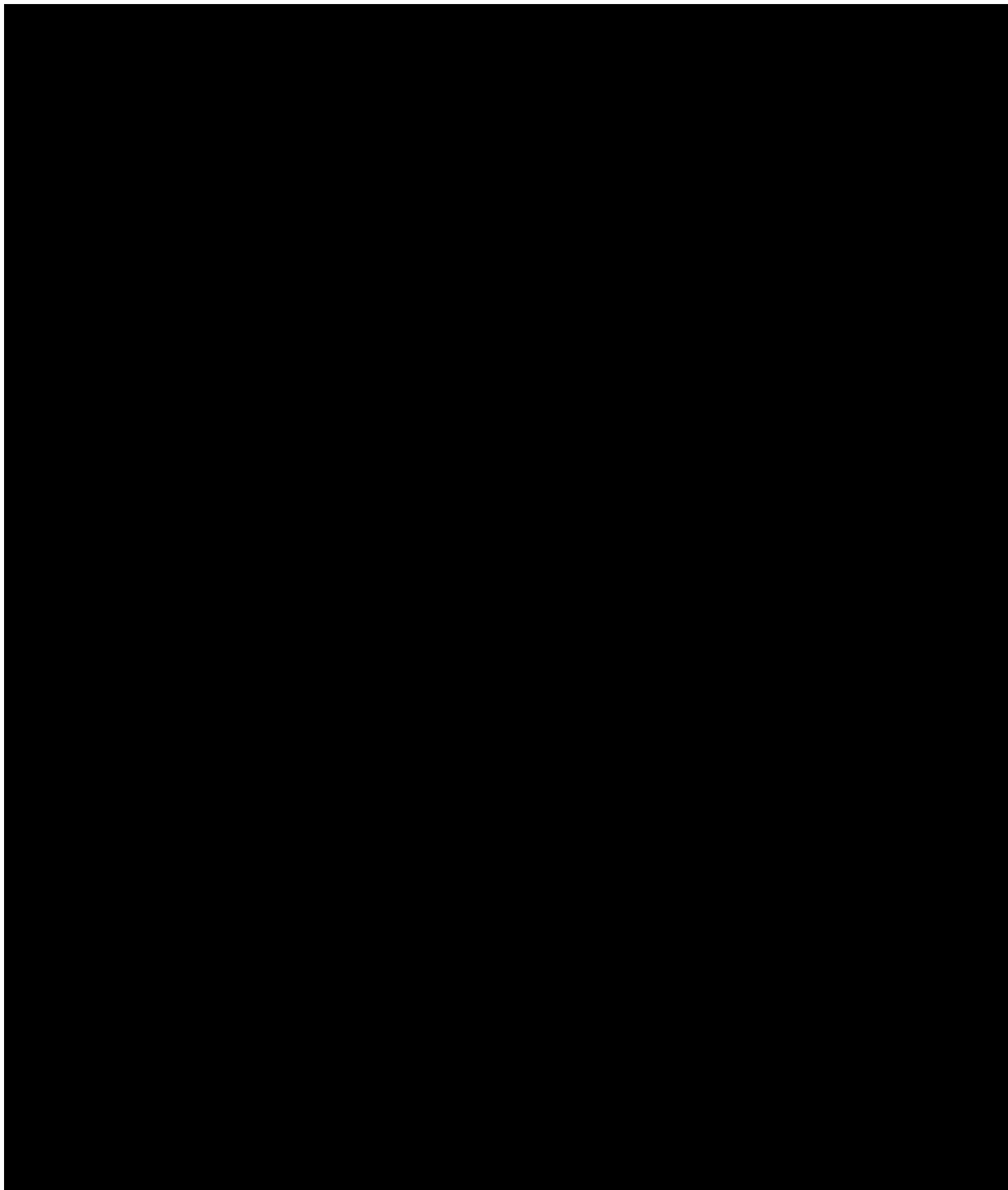
45%





Word Count	<i>Word Count: 993</i>
------------	------------------------

**Annex 3 – Supplier Goods/Services Quote (Provided as part of Insight’s Tender Bid)**









#### Annex 4 – Social Value Submission (Insight’s Response to Annex 6 of the ITT)

Theme	Outcomes	Ref	Measure and Description	Definitions	Unit	Social value Proxy	Quantity of Units	Total Social Value	Provide description here and demonstrate and detail exactly how this measure will be delivered during the contract.
Jobs: Promote Local Skills and Employmen	More opportunities for disadvantaged people	NT10	No. of apprenticeships on the contract that have either been completed during the year, or that will be supported by the organisation to completion in the following years - Level 2,3, or 4+	Apprenticeships and VQ	No. weeks	£176.80			





Theme	Outcomes	Ref	Measure and Description	Definitions	Unit	Social value Proxy	Quantity of Units	Total Social Value	Provide description here and demonstrate and detail exactly how this measure will be delivered during the contract.
Jobs: Promote Local Skills and Employmen	More opportunities for disadvantaged people	NT3	No. of employees (FTE) hired on the contract as a result of a recruitment programme that have been unemployed for a minimum of 6 months. Record the number of full time annual equivalent (FTE) employees taken on as a result of this contract that had been claiming Jobseeker's Allowance (JSA) or Universal Credit unemployment benefits for minimum of 6 months preceding the start of the employment contract.	N/A	No. people FTE	£15,085.95			



Theme	Outcomes	Ref	Measure and Description	Definitions	Unit	Social value Proxy	Quantity of Units	Total Social Value	Provide description here and demonstrate and detail exactly how this measure will be delivered during the contract.
Jobs: Promote Local Skills and Employment	Improved employability of young people	NT12/ NT13	No. of weeks spent on meaningful paid / unpaid work placements, pre-employment course or internships of a duration of no less than 1 week. Work placements indicate a temporary work experience within the company, for example working on junior-level tasks for the purpose of gaining experience and insight into the industry, or a more skill specific graduate position.	Work placement	No. weeks	£148.95			

Theme	Outcomes	Ref	Measure and Description	Definitions	Unit	Social value Proxy	Quantity of Units	Total Social Value	Provide description here and demonstrate and detail exactly how this measure will be delivered during the contract.
Social: Healthier, Safer and more Resilient Communities	More working with the Community	NT28	Donations for local community projects, third sector and civil society organisations. This could be a cash donation or the equivalent value of in kind contributions - e.g. paint, desks, ICT equipment or the use of office accommodation.	Community support	£ value	£1.00			





## Cisco Enterprise Agreement 3.0 Program Terms – End Users

These Cisco Enterprise Agreement 3.0 Program Terms – End Users (“**EA Program Terms**”) apply when You Order Suites and Add-Ons through the Cisco Enterprise Agreement 3.0 Buying Program (the “**EA Program**”). Capitalized terms, unless defined in these EA Program Terms, have the meaning in the General Terms.

### 1. Program Overview

- 1.1 **EA Program.** The EA Program provides You access to certain Software, Cloud Services, and Services offered as Suites and Add-Ons.
- 1.2 **Applicable Terms.** These EA Program Terms and the Buying Program Offer Descriptions govern the EA Program and are Supplemental Terms to the End User Terms that govern Your Use of the Suites and Add-Ons purchased under the EA Program (“**Purchased Suite(s)**”). These EA Program Terms must be signed and will be effective the earlier of (a) You placing Your Initial EA Order with an Approved Source, or (b) the date of signature of these EA Program Terms.

### 2. Purchases and Adjustments

- 2.1 **Ordering.** All purchases under the EA Program will be made through Your Approved Source and all pricing will be provided by Your Approved Source. Your first Order under these EA Program Terms must meet the minimum requirements for the EA Program (“**Initial EA Order**”). Following Your initial Full Commit Suite purchase in a Portfolio, You may only purchase additional Suites or Add-Ons within that Portfolio through the Approved Source that sold the initial Full Commit Suite within that Portfolio.
- 2.2 **Subsequent Purchases.** Provided there is at least 12 months remaining in the EA Term, Suites and Add-Ons purchased after Your Initial EA Order will be governed by these EA Program Terms and, by default, co-terminate with the purchases in the Initial EA Order.
- 2.3 **Separate Purchases.** The following scenarios must be covered under a new EA Program purchase subject to Cisco’s then-current Enterprise Agreement Program Terms - End Users or through a separate purchase outside of the EA Program: (i) Suites and Add-Ons purchased with less than 12 months remaining in the EA Term, (ii) Suites and Add-Ons with a desired Suite Term end date after the EA Term, or (iii) Embedded Software delivered within the last 12 months of or after the end of the EA Term.
- 2.4 **Payment Obligations and Growth.** You will pay for the EA Commitment for the EA Term and any increases in Use.

- (A) True Forward. Cisco has a process to periodically review, invoice, and adjust Entitlements for increases in Use above Your then-current Entitlement ("**True Forward**"). At True Forward, if Your Use of a Suite or Add-On is greater than Your then-current Entitlement for the measured Suite or Add-On, then (i) Cisco has the right to invoice for all associated charges for such increased Use over the applicable Entitlement prospectively through the remainder of the Suite Term, (ii) You will pay for all such charges, and (iii) Cisco will adjust Your Entitlement for that Suite or Add-On going-forward to the increased Use level.
- (1) General. During the Suite Term, the True Forward will, by default, be conducted at the annual anniversary of the Initial EA Order date.
- (2) Off-Cycle True Forward. If Your Use of a Suite or Add-On exceeds 115% of Your then-current Entitlement ("**Exceptional Growth**"), Cisco has the right to initiate an off-cycle True Forward at the next semi-annual anniversary of the Initial EA Order date in addition to Your annual True Forward.
- (B) Adjustments to True Forward Calculation. Certain Full Commit Suites are eligible for value shift, as specified in the Buying Program Offer Descriptions.
- (1) Intra Suite Value Shift. During a True Forward, the remaining value of any purchased but unused Software, Cloud Services, or Services in the applicable Purchased Suite will automatically be applied to offset fees for increased Use within the same Suite.
- (2) Cross Suite Value Shift. During a True Forward, for a Full Commit Suite, You may apply the remaining value in full or in part of (i) purchased but unused Software, Cloud Services, or Services and (ii) Software, Cloud Services, or Services previously Used that You agree to no longer Use, to offset amounts owed for increased Use in another eligible Suite in the same Portfolio. To take advantage of Cross Suite Value Shift You will need to: (i) have Ordered Suite(s) from the same Approved Source with the same Suite Term end date, and (ii) provide Your Approved Source with 60 days' notice before Your next annual True Forward anniversary.

2.5 **Price Predictability**. True Forward charges will be based on either a: (i) Not-to-Exceed Pricing for Full Commit Suites or (ii) fixed discount for applicable Partial Commit Suites or Add-Ons, in each case as provided to You by Your Approved Source. The pricing and discount terms for specific Suites and Add-Ons apply only to the Approved Source from whom You purchased such Suites and Add-Ons.

2.6 **Responsibility for Affiliates**. Your payment obligation will be based on the EA Commitment by You and any Affiliates that You have identified as participating in this EA Program. You remain responsible for all actions and omissions and payment of all charges incurred by You, any of Your Affiliates, or any other Authorized Users. In addition, You will provide Your Approved Source with an updated list of participating Affiliates to ensure compliance with the EA Program.

### 3. Term and Termination

3.1 **EA Term**. These EA Program Terms will remain in effect until expiration or termination of all the Suites and Add-Ons purchased in Your Initial EA Order ("**EA Term**").

3.2 Termination:

- (A) Either party may terminate these EA Program Terms (or Use of specific Suites or Add-Ons, as applicable) if the other party materially breaches the Applicable Terms, and that party does not cure the breach within 30 days of written notice from the non-breaching party. If You materially breach the Applicable Terms (including for non-payment of undisputed fees to the Approved Source), Cisco may also suspend Your access to the EA Program (including Use of specific Suites or Add-Ons, or

resources such as the Cisco EA Tool) after providing You notice and an opportunity to cure as set forth in this section.

- (B) Except as required by law or Section 3.2(a) above, these EA Program Terms and any Orders accepted under the EA Program may not be cancelled or terminated.

3.3 Consequences of Termination or Expiration of a Suite Term:

- (A) Upon expiration of the Suite Term or termination pursuant to Section 3.2(a), all rights to Use the affected Suites and Add-Ons, or the Cisco EA Tool and resources available as part of the Suites and Add-Ons, will terminate.
- (B) If You terminate for Cisco's uncured material breach, Cisco will provide a refund to Your Approved Source for the remaining pro rata portion of amounts prepaid to Cisco for the terminated Purchased Suites and attributable to the period after termination.
- (C) If Cisco terminates for Your uncured material breach, You will pay all unpaid fees through the end of the then-current Suite Term for all Purchased Suites terminated.

- 3.4 **Assignment and Transfer.** Neither these EA Program Terms, nor any right or obligation herein, may be assigned or transferred by a party (including under the Cisco Software Transfer and Re-licensing Policy) without the other party's prior written consent, which may not be unreasonably conditioned, withheld, or delayed. However, to continue providing You with the benefits of the EA Program, Cisco may assign or transfer its obligations (in whole or in part) upon written notice to You in the event of an acquisition of business assets to which these EA Program Terms relate. When validly assigned or transferred, these EA Program Terms will bind and inure to the benefit of the parties and their successors and assigns.

## 4. Delivery, Tax and Customs

- 4.1 **Delivery.** Cisco will make electronically delivered Software available to You and Your Affiliates in the transaction country of record and You are responsible for distributing such Software across Your organization. Software delivered on newly purchased Hardware will be made available to You and Your Affiliates at the address provided with the purchase order for the Hardware. For purchases of Hardware with Embedded Software, You must use the EA Tool during the setup of Your Cisco Enterprise Agreement.
- 4.2 **Embedded Software.** During the Suite Term, for Purchased Suites that include Embedded Software, the value of Embedded Software may be deducted from the purchase price of the related Hardware from Cisco to Your Approved Source. If You are required to pay an importation fee, Your jurisdiction may use the value of both the Hardware and Embedded Software to calculate the importation fee and related duties. Accordingly, the importation fee on the value of the combined products may be higher than if calculated solely using the price of the Hardware.

## 5. Interpretation

- 5.1 **Order of Precedence.** If there is any conflict between the EA Program Terms, the Buying Program Offer Descriptions, and the End User Terms, the order of precedence is: the Buying Program Offer Descriptions, these EA Program Terms, Offer Descriptions or Services Descriptions, and then the General Terms or equivalent written agreement between You and Cisco for accessing and using Software and Cloud Services. This order of precedence supersedes the order of precedence in the General Terms for Orders in the EA Program.
- 5.2 **Entire Agreement.** These EA Program Terms, together with the applicable Buying Program Offer Descriptions and End User Terms, are the complete agreement between the parties regarding the purchase of Software, Cloud Services, and Services under the EA Program and supersedes all prior or

contemporaneous communications, understandings, or agreements (whether written or oral).

## 6. Definitions

Term	Meaning
<b>Add-On</b>	An optional Software, Cloud Services, and Services offering that is available as an additional add-on purchase to an underlying Suite, as described in the Buying Program Offer Descriptions.
<b>Applicable Terms</b>	The EA Program Terms, Buying Program Offer Descriptions and End User Terms, as described in Section 1.2.
<b>Buying Program</b>	The description of EA Program features applicable to the Software, Cloud Services and Services in the
<b>Offer Descriptions</b>	EA Program available at the <a href="#">Offer Descriptions</a> site.
<b>Cisco EA Tool</b>	The applicable platform, website, tool, or portal that Cisco makes available to You under the EA Program from time to time to enable You to: (i) view and manage Your Entitlement and Use of the Suites and Add-Ons; and (ii) access information about the EA Program.
<b>Cross Suite Value Shift</b>	The ability to shift value across eligible Suites as described in Section 2.4(b)(2).
<b>EA Commitment</b>	(i) The initial Entitlement under Your Initial EA Order, (ii) additional Entitlements associated with subsequent purchases of Suites and Add-Ons, and (iii) increases in Use.
<b>Embedded Software</b>	Software that is delivered on newly purchased Hardware.
<b>End User Terms</b>	As specified in the Buying Program Offer Descriptions:  (i) For Cisco Software and Cloud Services, the <a href="#">General Terms</a> (including applicable <a href="#">Offer Descriptions</a> ), or equivalent written agreement between You and Cisco for accessing and using Software and Cloud Services; and (ii) For Services, the applicable <a href="#">Service Descriptions</a> .
<b>Entitlement</b>	The type, quantity or value, and duration of Suites and Add-Ons that You have committed to acquire (or previously acquired and agreed to cover under the EA Program), as adjusted (e.g., as a result of a True Forward).
<b>Full Commit Suite</b>	A Suite acquired on terms (including duration, price, and quantities) that fulfil the minimum requirements for a 'Full Commit Suite', as set out in the Buying Program Offer Descriptions.
<b>Intra Suite Value Shift</b>	The ability to shift value within an eligible Suite, as described in Section 2.4(b)(1).
<b>Not-to-Exceed Pricing</b>	Pricing model that (i) includes a maximum price and (ii) allows for lower prices if applicable list price decreases.
<b>Partial Commit Suite</b>	A Suite acquired in addition to a corresponding Full Commit Suite, that does not meet the minimum eligibility requirements for a Full Commit Suite.

<b>Portfolio</b>	A standardized grouping of Suites and optional Add-Ons.
<b>Services</b>	Services for the applicable Hardware, Software, or Cloud Services corresponding to the Purchased Suite.
<b>Suite</b>	A defined combination of Software, Cloud Services, and Services made available under the EA Program.
<b>Suite Term</b>	With respect to each Purchased Suite, the duration of the Purchased Suite, commencing on the earliest date any Software, Cloud Services and Services in the Purchased Suite is available for Your Use.
<b>Use</b>	To download, install, activate, provision, enable, or otherwise access or have available Suites and Add- Ons under the EA Program.
<b>You or Your</b>	The individual or legal entity purchasing the Software, Cloud Services, and Services under the EA Program.

## Terms and Conditions Acceptance

I have read the terms and conditions above and understand that if an order is placed, these terms and conditions will apply to the purchased suites.

End User Acceptance

## Annex 6 – Insight Product Payment Agreement



### PRODUCT PAYMENT AGREEMENT

**TO OUR VALUED CUSTOMER:** This Product Payment Agreement ("PPA") has been written in "Plain English". When we use the words **you** and **your** in this PPA, we mean **you, our customer**, which is the **Customer** indicated below. When we use the words **we, us**, and **our** in this PPA, we mean **Insight Direct (UK) Limited** a company incorporated in England under registration number 02579852 whose registered address is Insight Campus Terry Street, Sheffield, S9 2BU.

#### **CUSTOMER INFORMATION**

*Customer Name*

**COMPETITION AND MARKETS AUTHORITY**

*Billing Address*

The Cabot, 25 Cabot Square, London, E14 4QZ

*Product Location (if different from above)*

*Accounts Payable Contact*

#### **PRODUCTS AND SERVICES DESCRIPTION**

**Quantity**

**Description**

**Serial Number**

Please refer to Schedule

	Initial Payment Term (Months)	Installment Payment	You agree to pay the Installment Payments on the due dates below (the "Installment Payment Dates"):		
<b>TERMS AND PAYMENT SCHEDULE</b>	<b>36 Months</b>		A) Total Advance Installment Payment:  B) VAT on the deliverable  C) One-time Documentation Fee:  D) Total of A + B + C:		<b>PLUS APPLICABLE TAXES</b>

#### **TAXES**

You are required to pay any value added, sales, use and other taxes related to this PPA and/or the Products. (See Section 5 of this PPA.) If you are tax-exempt, you agree to furnish us with satisfactory evidence of your exemption.

---

## PRODUCT PAYMENT TERMS AND CONDITIONS

**BY SIGNING THIS PPA: (i) YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THE TERMS AND CONDITIONS OF THIS PPA; (ii) YOU AGREE THAT YOU CANNOT TERMINATE OR CANCEL THIS PPA OR RETURN THE PRODUCT TO US, AND YOU HAVE AN UNCONDITIONAL OBLIGATION TO MAKE ALL PAYMENTS DUE UNDER THIS PPA, AND YOU CANNOT ABATE, WITHHOLD, SET OFF, DELAY, COUNTERCLAIM AGAINST OR REDUCE SUCH PAYMENTS FOR ANY REASON; (iii) YOU WILL USE THE PRODUCT ONLY FOR BUSINESS PURPOSES AND FULLY IN ACCORDANCE WITH THE APPLICABLE SOFTWARE PUBLISHER END USER LICENCE AGREEMENT AND OTHER APPLICABLE PRODUCT TERMS OF USE; (iv) YOU WARRANT THAT THE PERSON SIGNING THIS PPA HAS THE NECESSARY AUTHORITY TO DO SO; (v) YOU CONFIRM THAT YOU DECIDED TO ENTER INTO THIS PPA RATHER THAN PURCHASE THE PRODUCT FOR THE TOTAL CASH PRICE; (vi) YOU AGREE THAT THIS PPA WILL BE GOVERNED BY AND SHALL BE CONSTRUED IN ACCORDANCE WITH THE LAWS OF ENGLAND AND WALES AND YOU SUBMIT TO THE EXCLUSIVE JURISDICTION OF THE COURTS OF ENGLAND; AND (vii) YOU AGREE THAT THE TERMS AND CONDITIONS OF THIS PPA MAKE UP THE ENTIRE AGREEMENT BETWEEN YOU AND US REGARDING YOUR PAYMENT OBLIGATIONS TO US AND OUR OBLIGATIONS TO YOU AND TAKE PRECEDENCE OVER ANY ALTERNATIVE OR CONTRADICTORY TERMS WHETHER IN A PUBLIC SECTOR FRAMEWORK OR CALL OFF CONTRACT, PURCHASE AGREEMENT OR ANY STANDARD OR BOILER PLATE TERMS AND CONDITION REFERENCED IN A PURCHASE ORDER OR OTHERWISE; (viii) YOU AGREE TO IMMEDIATELY RAISE AND PROVIDE TO INSIGHT A PURCHASE ORDER IN RESPECT OF ALL OF THE PRODUCTS AS QUOTED TO YOU.**

**1. DEFINITIONS.** "Affiliate" means, in relation to a Party, any entity that directly or indirectly, controls, is controlled by, or is under common control of or with a Party to this PPA. For purposes of this definition, "control" means having 50% or more of the outstanding equity interests or having, by contract or otherwise, the right and ability to direct management and policies; "Hardware" means the IT product available for purchase through Insight under this PPA; "Product(s)" means Hardware, Software and its related integration, maintenance and support, and third-party branded and "Skuable Services" (meaning standard third-party services that are sold with a Stock Keeping Unit (SKU) code); "Sanctioned Person" means any person, whether or not having a legal personality: (a) listed on any list of designated persons in application of Sanctions; (b) located in, or organised under the laws of, any country or territory that is subject to comprehensive Sanctions; (c) directly or indirectly owned or controlled, as defined by the relevant Sanctions, by a person referred to in (a) or (b) above; or (d) which otherwise is, or will become with the expiry of any period of time, subject to Sanctions; "Sanctions" means any economic or financial sanctions, trade embargoes or similar measures enacted, administered or enforced by any of the following (or by any agency of any of the following): (a) the United Nations; (b) the United States of America; (c) the European Union or any present or future member state thereof; or (d) the United Kingdom; and "Software" means software product and its related maintenance and support available for purchase through Insight under this PPA. We will not accept returns of Hardware. Hardware returns for replacement may be accepted by the manufacturer under the applicable manufacturer warranty (if any).

**2. PAYMENT OF PRODUCTS; DELIVERY AND ACCEPTANCE.** You agree to pay the Installment Payments associated with the Product described on the first page of this PPA on an extended payment basis in accordance with the terms and conditions shown in this PPA. With regard to Software: we shall arrange for the delivery of a license key, to enable you to download, access and install the Software (which are your responsibilities). You agree to promptly, and in any case within three (3) days following shipment of the software publisher's welcome email (containing the license key and/or portal access instructions), inspect the Software and deliver to us a signed copy of the Delivery and Acceptance Certificate in the form scheduled hereto. With regard to Hardware: upon delivery of the Hardware, you agree to promptly, and in any case within three (3) days following delivery of the Hardware, deliver to us a signed copy of the Delivery and Acceptance Certificate in the form scheduled hereto. By signing the Delivery and Acceptance Certificate or in the case of any failure by you to return the Delivery and Acceptance Certificate in the required three (3) day timescale shall signify your irrevocable acceptance of the Product. The first Installment Payment will be due on the first day of the month following delivery of the Product in accordance with this Section 2, and the remaining Installment Payments will be due on the first day of each subsequent calendar year (or such other time period specified on the front of this PPA) designated by us. No payment due hereunder may be prepaid prior to its scheduled due date. We will not accept returns of Hardware. Hardware returns for replacement may be accepted by the manufacturer under the applicable manufacturer warranty (if any).

You agree to make all payments required under this PPA to us in line with the following:

Payment shall be made on receipt of a valid invoice and in alignment with the Installment Payment Dates.

Our preferred payment collection method is Direct Debit. You agree to set up and make all Installment Payments to Insight Direct (UK) Ltd by Direct Debit on the Installment Payment Dates, and you agree to set up a Direct Debit mandate in respect of the foregoing in line with our directions. If an alternative payment method is otherwise agreed (in writing by us) payment shall be made by you to the following in accordance with the Installment Payment Dates:

Bank: If funding in GBP: Bank of America NA London, Sort Code: 16-50-50, Account Number: 66210015, IBAN: GB93 BOFA 16505066 2100 15.

If any Installment Payment or other amount payable under this PPA is not paid within **3** days of its due date, you will pay us a late charge on the overdue late payment of 6% per annum above the base rate of Barclays Bank PLC. If you are required (either by law, regulation or otherwise) to make a deduction or withholding from any payment of an Installment Payment, you shall pay us an amount which, after making such deduction or withholding, leaves an amount equal to the payment that would have been due if no deduction or withholding had been required.



**3. NO WARRANTIES; LIABILITY.** We are remitting payment to a vendor to enable your acquisition of the Product on an "AS-IS" basis. **YOU ACKNOWLEDGE THAT WE DO NOT PUBLISH OR DIRECTLY LICENSE THE SOFTWARE OR MANUFACTURE THE HARDWARE, AND WE ARE NOT AN AGENT FOR OR OTHERWISE REPRESENT THE PUBLISHER OR LICENSOR OF THE SOFTWARE OR THE MANUFACTURER OF THE HARDWARE, OR THE PROVIDER OF THE SERVICES, AND YOU HAVE SELECTED THE PRODUCTS BASED UPON YOUR OWN JUDGMENT. WE MAKE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR OTHERWISE IN RESPECT OF THE PRODUCT. YOU AGREE THAT REGARDLESS OF CAUSE, WE ARE NOT RESPONSIBLE FOR AND YOU WILL NOT MAKE ANY CLAIM AGAINST US FOR ANY DAMAGES, WHETHER CONSEQUENTIAL, DIRECT, SPECIAL, OR INDIRECT.**

**NOTWITHSTANDING ANY OTHER PROVISION IN THIS PPA, THE LIABILITY OF THE PARTIES SHALL NOT BE LIMITED IN ANY WAY IN RESPECT OF THE FOLLOWING: (A) DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE, (B) FRAUD OR FRAUDULENT MISREPRESENTATION, AND (C) ANY OTHER LOSSES WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW.**

**4. LICENSE AGREEMENT; TERMS OF USE.** YOU ACKNOWLEDGE AND AGREE THAT YOU HAVE READ AND RECEIVED THE APPLICABLE SOFTWARE PUBLISHER END USER LICENSE AGREEMENT RELATED TO THE SOFTWARE ("LICENSE AGREEMENT"). YOU ARE THE LICENSEE UNDER THE LICENSE AGREEMENT AND YOU AGREE TO PERFORM ALL OF THE OBLIGATIONS OF THE LICENSEE UNDER THE LICENSE AGREEMENT, AND ONLY USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS OF THE LICENSE AGREEMENT. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT WE HAVE NOT ASSUMED ANY OF THE SOFTWARE PUBLISHER'S OR LICENSOR'S OBLIGATIONS UNDER THE LICENSE AGREEMENT AND THAT WE SHALL HAVE NO LIABILITY FOR THE PERFORMANCE OF THE SOFTWARE OR THE SOFTWARE PUBLISHER'S OR LICENSOR'S OBLIGATIONS UNDER THE LICENSE AGREEMENT. We may inspect the Software and/or Hardware at any reasonable time.

**5. TAXES AND FEES.** You will pay when due, either directly to us or upon our demand, all taxes, fines and penalties relating to this PPA, the License Agreement or the Product that are now or in the future assessed or levied by any state, local or government authority. Installment Payments are exclusive of VAT. The value added tax or any other sales tax related to the Product will be calculated by us and added to each Installment Payment. We do not have to contest any taxes, fines or penalties.

**6. LOSS OR DAMAGE.** As between you and us, following delivery, you are responsible for any loss, theft, destruction of, or damage to the Product (collectively "Loss") from any cause at all, whether or not insured. You are required to make all Installment Payments even if there is a Loss. You must notify us in writing immediately of any Loss. Upon the occurrence of a Loss you will immediately pay us the amounts specified in Section 10(b) below. Upon our full receipt of all amounts referred to in Section 10(b) below together with any other amounts due under this PPA you will no longer be obligated to make the remaining Installment Payments under this PPA.

**7. TITLE TO THE SOFTWARE; INTEREST IN RIGHTS.** You will keep the Software free of all liens and encumbrances. The Software publisher (or Licensor as applicable) shall be the owner and hold title to the Software. You acknowledge that we have paid the license fee associated with the acquisition of your rights under the License Agreement. To secure your payment and performance of your obligations under this PPA, you hereby grant to us and our successors and assigns a continuing security interest in the following: (a) all rights with respect to the Software and all rights to payment thereunder relating to any refund, indemnification, and/or abatement to which you are or become entitled, no matter how or when arising, whether such rights are classified as accounts, general intangibles, or otherwise; and (b) all proceeds of the foregoing.

**8. DELIVERY; TITLE TO HARDWARE.** We will use reasonable endeavours to dispatch goods by the date agreed with you, but do not accept liability for failure to deliver within the stated time. Delivery is deemed to take place when the goods are delivered to the Customer's nominated address, whereupon the risks of loss, breakage and all damage and all other risks shall pass to you. Any freight costs shall be paid by us and charged back to you.

**9. DEFAULT.** Each of the following is a "Default" under this PPA: (a) you fail to pay any Installment Payment or any other payment when it becomes due; (b) you do not perform any of your other obligations under the License Agreement and/or other Product Terms of Use, this PPA, or in any other agreement with us or with any of our Affiliates and this failure continues for 10 days after we have notified you of it; (c) you cease or threaten to cease to carry on your business; (d) if this PPA terminates for any reason; (e) you are unable to pay your debts as they fall due or are declared bankrupt or apply for a moratorium of payments or make or propose to make any arrangement with your creditors or a liquidator, administrator, administrative receiver or receiver is appointed over you or any of your assets; (f) we determine that any one of your representations and warranties outlined in Section 13 below are incorrect; (g) without our prior written consent, there is a change in the majority of shareholder voting rights or you merge or consolidate with any other entity and you are not the survivor of such merger or consolidation; (h) any guarantor of this PPA dies, does not perform its obligations under the guarantee, or becomes subject to one of the events listed in sub-clause (c), (e) or (g) above; or (i) there is a material adverse change to the financial or business position of you which, in the reasonable opinion of us, will (or is likely to) affect the ability of you to pay your debts as they become due and/or perform your obligations under this SPA. Should a Default event occur or be likely to occur, you shall notify us in writing immediately (and in any event by the following business day) after becoming aware of such a Default event and comply with our lawful instructions therewith.

**10. REMEDIES.** If a Default occurs, we may do one or more of the following: (a) we may cancel or terminate this PPA or any or all other agreements that we have entered into with you; (b) we may require you to immediately pay us on demand, as compensation for loss of our bargain and not as a penalty, a sum equal to: (i) all unpaid Installment Payments for the remainder of the term of this PPA, plus (ii) all other amounts due that are in arrears or that become due under this PPA; (c) foreclose the security interest in your

rights with respect to the Products; (d) cancel, terminate, or cause the Publisher or Licensor of the Software to cancel and/or terminate all licenses for Software granted to you, (e) cancel, terminate, suspend or withhold or cause the Publisher or Licensor or Manufacturer of the Product to cease providing maintenance and/or support for the Product; (f) upon termination of your rights to use any or all of the licenses for the Software you shall deliver to us the terminated Software and all related documentation, and copies thereof, and shall promptly certify to us in writing that all terminated Software has been removed from the hardware upon which it was installed, and that any copies not returned to us have been destroyed; (we shall have the right to enter into your premises for the purpose of verifying that all terminated Software has been removed from your hardware); (g) require the return of any Hardware Product and if such items are not returned to Us promptly, we may enter into your premises for the purpose of recovery of such Hardware items; and (h) we may exercise any other right or remedy available at law or in equity. Your obligations to pay the Installment Payments shall continue, notwithstanding any termination of this PPA by either party. No failure or delay on our or our assignee's part to exercise the forgoing rights and remedies shall operate as a waiver thereof. **You agree to reimburse all of our costs of enforcing our rights against you, including reasonable attorneys' fees.**

**11. ASSIGNMENT. YOU MAY NOT ASSIGN, SELL, CHARGE, DISPOSE OF, NOVATE OR OTHERWISE TRANSFER OR SUBLICENSE THE PRODUCT OR YOUR INTEREST IN THIS PPA OR ANY RIGHT OR OBLIGATION HEREUNDER.** We may, without notifying you, sell, assign, novate or otherwise transfer any of our rights and/or benefits in this PPA. We shall be entitled to assign our rights and benefits in and to any payments our sums due and to become due under this PPA. The assignee shall have the same rights and benefits that we have now under this PPA but not our obligations. The rights and benefits of any assignee will not be subject to any claims, defenses, withholding or set-off that you may have against us.

You shall promptly pay and reimburse any of our assignees for all costs, fees, and expenses (including, without limitation, reasonable legal costs and expenses) incurred by any such assignee in enforcing the assigned rights in respect of this PPA.

The parties agree to the confidentiality and data protection provisions contained in the Schedule hereto. To the extent that any assignee is processing any personal data relating to you, such processing shall be in accordance with fair processing notice for data protection purposes, a copy of which is located here: <https://www.uk.insight.com/en-gb/knowledge-base/policies/privacy-statement>

**12. CREDIT INFORMATION.** You acknowledge that, for the purposes of any assignment referred to in Section 11, our assignee or us may be required to conduct due diligence on you and your directors, trustees, employees and beneficial owners, for the purpose of processing, managing, financing and/or funding of this PPA. Such due diligence may comprise identity verification, politically exposed persons screening, sanctions screening, fraud checks and credit checks, to the extent these are required by the laws of any jurisdiction to which our assignee or us may be subject and/or as a matter of prudent risk management in accordance with industry practice. You agree to provide any documentation reasonably requested by us in order to permit us or our assignee to conduct such due diligence, and acknowledge that your information, including personal information about your directors, trustees, employees and beneficial owners, may also be collected directly from public registers and other publicly available sources. You warrant that you will make your directors, trustees, employees and beneficial owners aware of the collection and processing of personal information in connection with such due diligence activities and that you will obtain their consent to the same (to the extent this is required by applicable privacy related laws).

**YOU AUTHORIZE US OR ANY OF OUR AFFILIATES OR ASSIGNS TO OBTAIN CREDIT BUREAU REPORTS, AND MAKE OTHER CREDIT INQUIRIES THAT WE DETERMINE ARE NECESSARY. ON WRITTEN REQUEST, WE WILL INFORM YOU WHETHER WE HAVE REQUESTED A CONSUMER CREDIT REPORT AND THE NAME AND ADDRESS OF ANY CONSUMER CREDIT REPORTING AGENCY THAT FURNISHED A REPORT. YOU ACKNOWLEDGE THAT WITHOUT FURTHER NOTICE WE MAY USE OR REQUEST ADDITIONAL CREDIT BUREAU REPORTS TO UPDATE OUR INFORMATION SO LONG AS YOUR OBLIGATIONS TO US ARE OUTSTANDING.**

**13. YOUR REPRESENTATIONS.** You represent, warrant and covenant to us that as of the date of this PPA and for so long as this PPA shall remain in effect: (a) you are duly organized, validly existing and in good standing under applicable law; (b) you have the power and authority to enter into this PPA; (c) all agreements with us including this PPA are enforceable against you in accordance with their terms and do not violate or create a default under any instrument or agreement binding on you; ; (d) you are a non-ministerial government department organised under the laws of England and Wales with a registered office at The Cabot, 25 Cabot Square, London, E14 4QZ a company registration number of n/a ; and a VAT registration number of GB888850063; (e) you (including any guarantor, if applicable) are familiar with the provisions of all applicable Anti-Corruption Laws (meaning the U.S. Foreign Corrupt Practices Act, the U.K. Bribery Act and other analogous anti-corruption legislation in other jurisdictions in which Customer conducts business or which otherwise apply to Customer collectively, and with related regulations), and shall not in connection with any Fundamental Agreement (meaning, collectively, this PPA, the Delivery and Acceptance Certificate and all other related instruments and documents): (i) make any improper payment or transfer anything of value, offer, promise or give a financial or other advantage or request to, or agree to receive or accept a financial or other advantage from, either directly or indirectly, any government official or government employee (including employees of a government corporation or public international organization) or to any political party or candidate for public office or to any other person or entity with an intent to obtain or retain business or otherwise gain an improper business advantage; or (ii) take any action which would cause us to be in violation of any Anti-Corruption Laws; (f) you and all your Affiliates (including any guarantor, if applicable) shall not export, re-export, or transfer any Product or source code or any direct product thereof to a prohibited destination, or to nationals of proscribed countries wherever located, without prior authorization from the United States and other applicable governments; (g) you shall comply with all disclosure, reporting and other obligations to which you are or may become subject under the terms of The Foreign Account Tax

Compliance Act ("FATCA") and any United Kingdom legislation which implements or is substantially equivalent to FATCA in the United Kingdom; (h) you and all your Affiliates do not use any software or technology, technical data, or technical assistance related thereto or the products thereof in the design, development, or production of nuclear, missile, chemical, or biological weapons or transfer the same to a prohibited destination, or to nationals of proscribed countries wherever located, without prior authorization from the United States and other applicable governments; and (i) you and your Affiliates (including any guarantor, if applicable) are not designated by the United States government or any other applicable government as entities with which transacting business without the prior consent of such government is prohibited; (j) for all Products that fall under the WEEE Regulations, you shall ensure you follow the Producer (manufacturer) directions for disposal and recycling thereof. You agree to provide us advance written notice of any change in any of the representations and covenants set forth in clauses (d) through (j) of this Section and will promptly notify us if it becomes aware of any violation of the representations and covenants set forth in clause (e) of this Section.

#### **14. SANCTIONS.**

(a) You represent that neither you nor any of your Affiliates, nor, to the best of your knowledge, any of your directors, officers, employees or agents is a Sanctioned Person. This representation shall be deemed to be repeated at all times until the termination of this Agreement.

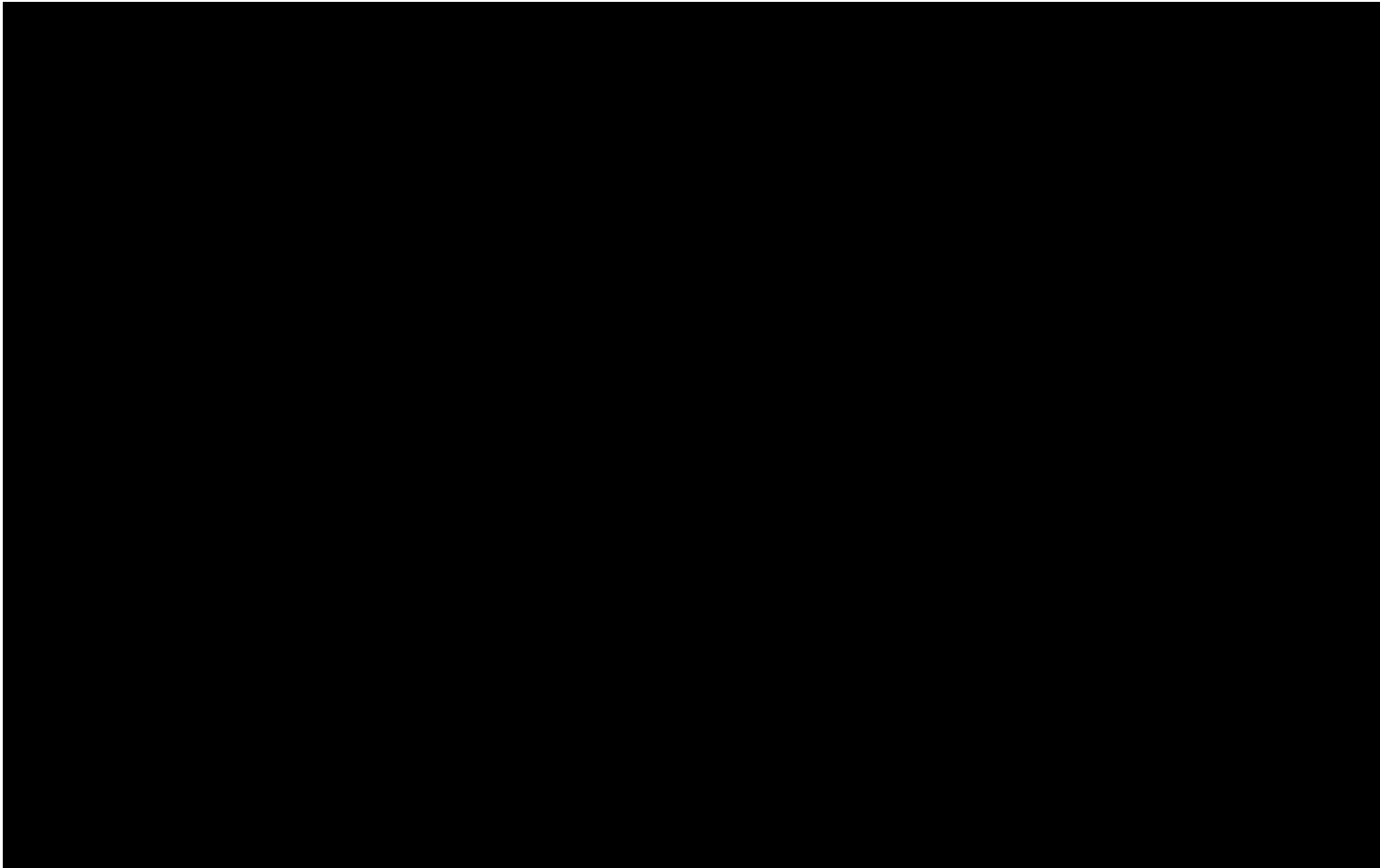
(b) You shall not, directly or indirectly, use the proceeds of the facility or allow these proceeds to be used (or lend, contribute or otherwise make available such proceeds to any person) to fund, participate or contribute to, any activities or business of, with or related to (or otherwise to make funds available to or for the benefit of) any person who is a Sanctioned Person.

(c) You shall ensure that you shall not use any revenue or benefit derived from any activity or dealing with a Sanctioned Person for the purpose of discharging amounts owing to us in respect of the Products. You shall implement and maintain appropriate safeguards designed to prevent any action that would be contrary to paragraph (a) or (b) above.

(d) You shall, and shall procure that each your Affiliates will, promptly upon becoming aware of the same, supply to us details of any claim, action, suit, proceedings or investigation against you with respect to Sanctions.

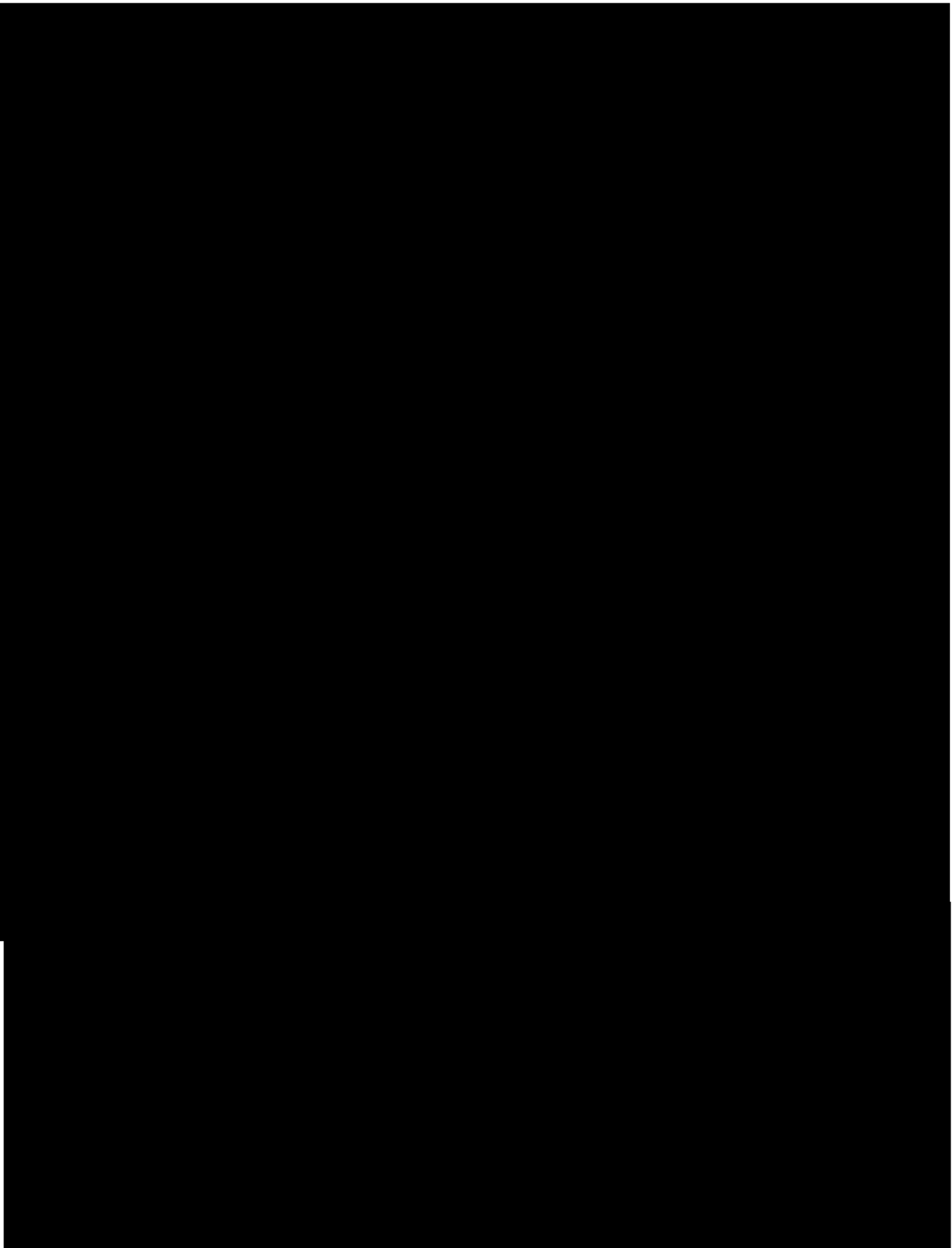
**15. MISCELLANEOUS.** This PPA is not binding on us until we sign it. Any change in any of the terms and conditions of this PPA must be in writing and signed by us. If we delay or fail to enforce any of our rights under this PPA, we will still be able to enforce those rights at a later time. If any term or provision of this PPA shall to any extent be held to be invalid or unenforceable the remainder of this PPA shall remain valid and shall be enforceable to the extent permitted by law. All notices shall be given in writing by the party sending the notice and shall be effective when deposited in the mail, addressed to the party receiving the notice at its address shown on the front of this PPA (or to any other address specified by that party in writing) with postage prepaid. All of our rights and indemnities will survive the termination of this PPA. It is the express intent of the parties not to violate any applicable usury laws or to exceed the maximum amount of time, price differential or interest, as applicable, permitted to be charged or collected by applicable law, and any such excess payment will be applied to Installment Payments in inverse order of maturity, and any remaining excess will be refunded to you. If you do not perform any of your obligations under this PPA, we have the right, but not the obligation; to take any action or pay any amounts that we believe are necessary to protect our interests. You agree to reimburse us immediately upon our demand for any such amounts that we pay. If more than one end user has signed this PPA, each of you agree that your liability is joint and several. This PPA is not regulated by the Consumer Credit Act 1974 (as amended).

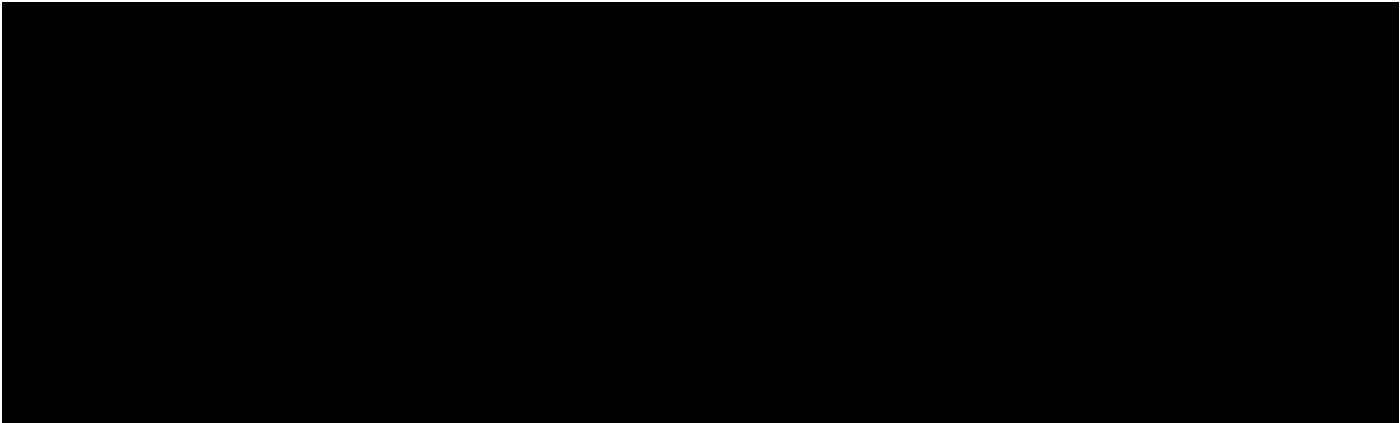
**NOTICE: IF YOU ARE TRANSMITTING THIS PPA TO US BY FACSIMILE OR ELECTRONIC TRANSMISSION, THE FACSIMILE OR PDF COPY OF THIS PPA AS RECEIVED BY US SHALL BE BINDING ON YOU AS IF IT WERE MANUALLY SIGNED BY YOU. HOWEVER, NO FAX OR OTHER VERSION OF THIS PPA SHALL BECOME BINDING AGAINST US UNTIL ELECTRONICALLY OR MANUALLY SIGNED BY US AND, IF YOU HAVE SIGNED AND TRANSMITTED THIS PPA TO US BY FACSIMILE OR EMAIL TRANSMISSION, YOU AGREE TO DELIVER TO US A COPY OF THIS PPA WITH YOUR ORIGINAL SIGNATURE. YOU AGREE THAT THE VERSION OF THIS PPA ELECTRONICALLY OR MANUALLY SIGNED BY US SHALL CONSTITUTE THE ORIGINAL OF THIS PPA FOR ALL PURPOSES. NO SECURITY INTEREST IN THIS PPA MAY BE CREATED THROUGH THE TRANSFER AND POSSESSION OF ANY COPY OR COUNTERPART HEREOF EXCEPT THE COPY WITH OUR ORIGINAL SIGNATURE. YOU AGREE THAT (i) YOU HAVE HAD A SUFFICIENT OPPORTUNITY TO READ AND REVIEW THE TERMS OF EACH PROVISION OF THIS PPA; (ii) YOU HAVE RECEIVED ALL OF THE PAGES OF THIS PPA (PLUS ANY SCHEDULE, ADDENDUM OR EXHIBIT HERETO) AND, IF APPLICABLE, THE GUARANTEE, AND THAT ALL OF SUCH PAGES AND OTHER DOCUMENTS ARE CLEAR AND LEGIBLE; AND (iii) THIS PPA IS COMPLETE AND THAT NONE OF THE PROVISIONS ARE MISSING OR ILLEGIBLE. YOU HEREBY WAIVE NOTICE OF OUR ACCEPTANCE OF THIS PPA AND WAIVE RECEIPT OF A COPY OF THE ACCEPTED PPA.**



## **Confidential Information and Data Protection Schedule to the PPA**

- (1) Each party shall preserve the confidentiality of all confidential information of the other which it receives, keep such information secure and protected against theft, damage, loss or unauthorised access, and not use such information for any purpose except as contemplated by the PPA. Moreover, each party shall ensure that such obligations are observed by its employees, officers, agents, contractors and partners. These obligations shall survive the variation, renewal or termination of the PPA for a period of three years but shall not apply to information which is already in or subsequently comes into the public domain through no fault of the recipient.
- (2) Each party shall process personal data in accordance with applicable data protection legislation (including the General Data Protection Regulation ((EU) 2016/679) (GDPR), the Data Protection Directive (95/46/EC), and any national implementing laws, regulations and secondary legislation including the UK Data Protection Act 2018) as amended from time to time (the "Data Protection Legislation"). Terms used throughout this clause including "data controller", "data processor", "data subject", "personal data" and "processing" are as defined in the Data Protection Legislation.
- (3) Personal data processing will be accomplished through electronic and non-electronic means, for the purpose of these terms and conditions. Customer is responsible for obtaining the consent of all Customer related data subjects whose personal data is provided to or otherwise made available to us pursuant to these terms and conditions or any order. Customer authorises Insight to engage subprocessors to the extent required for the performance of these terms and conditions and/or any order. Insight shall in respect of any personal data of the Customer processed under these terms and conditions, maintain such personal data under appropriate, commercially reasonable and sufficient technical and organisational security measures to protect such personal data or information and both Parties warrant to have taken all appropriate registrations under Data Protection Legislation. Customer authorises Insight to transfer and (sub)process any personal data outside of the European Economic Area (EEA) in order to perform these terms and conditions and/or the orders, other legal obligations and/or for Insight's other legitimate interests, provided that such transfer is made in accordance with Data Protection Legislation. Transfers outside of the EEA made within the Insight group of companies will be made under a legal framework compliant with the Data Protection Legislation such as the Privacy Shield or the European Commission approved Model Contract Clauses. Insight's Privacy Policy (available on request and on our website [www.UK/Insight.com](http://www.UK/Insight.com)) shall apply to orders placed. Notwithstanding any other provision of these terms and conditions, Customer agrees that Insight shall not be considered a data processor or data controller or in any other way have any responsibilities or liability (and the Customer holds Insight harmless) in respect of the processing of personal data pursuant to a product or service (including cloud service) provided by a third party supplier of product or services transacted by Insight and where Insight is not processing such data. Such processing of personal data shall be subject to the arrangements and contract or license terms entered into directly between Customer and the third party provider.







Adobe Acrobat Sign





Adobe Acrobat Sign