**DPS Schedule 6 (Order Form Template and Order Schedules)**

**Order Form**

ORDER REFERENCE: CCZZ21A59

THE BUYER: **Cabinet Office**

BUYER ADDRESS : Redacted Text Under FOIA Section 40, Personal Information

THE SUPPLIER: **Global Disability Innovation Hub C.I.C**

SUPPLIER ADDRESS:Redacted Text Under FOIA Section 40, Personal Information

REGISTRATION NUMBER:Redacted Text Under FOIA Section 40, Personal Information

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 28th October 2022

.

It’s issued under the DPS Contract with the reference number RM6126 for the provision of Assistive Technology Needs & Capacity Assessment Research

ORDER INCORPORATED TERMS

The following documents are incorporated into this Order 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 Order Special Terms and Order Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6126
3. DPS Special Terms
4. The following Schedules in equal order of precedence:

* Joint Schedules for RM6126
  + Joint Schedule 2 (Variation Form)
  + Joint Schedule 3 (Insurance Requirements)
  + Joint Schedule 4 (Commercially Sensitive Information)
  + Joint Schedule 6 (Key Subcontractors)
  + Joint Schedule 10 (Rectification Plan)
  + Joint Schedule 11 (Processing Data)
  + Joint Schedule 12 (Supply Chain Visibility)
* Order Schedules for CCZZ21A59
  + Order Schedule 1 (Transparency Reports)
  + Order Schedule 2 (Staff Transfer)
  + Order Schedule 3 (Continuous Improvement)
  + Order Schedule 4 (Order Tender)
  + Order Schedule 5 (Pricing Details)
  + Order Schedule 7 (Key Supplier Staff)
* Order Schedule 8 (Business continuity and disaster recovery)
  + Order Schedule 9 (Security)
  + Order Schedule 14 (Service Levels)
  + Order Schedule 20 (Order Specification)

1. CCS Core Terms (DPS version) v1.0.3
2. Joint Schedule 5 (Corporate Social Responsibility) RM6126
3. Order Schedule 4 (Order Tender) as long as any parts of the Order 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 Order Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

ORDER SPECIAL TERMS

Cabinet Office Security Schedule (Annex A Security Management - Assurance)

ORDER START DATE: 8th November 2022

ORDER EXPIRY DATE: 7th March 2023

ORDER INITIAL PERIOD: 4 months

DELIVERABLES

See details in Order Schedule 20 (Order Specification)

MAXIMUM LIABILITY

The limitation of liability for this Order 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 £182, 854.00 (excluding VAT).

ORDER CHARGES

See details in Order Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

Invoice BACS payments – on completion of milestones

BUYER’S INVOICE ADDRESS:

Redacted Text Under FOIA Section 40, Personal Information

Email: Redacted Text Under FOIA Section 40, Personal Information

Address: Redacted Text Under FOIA Section 40, Personal Information

BUYER’S AUTHORISED REPRESENTATIVE

Name: Redacted Text Under FOIA Section 40, Personal Information

Role: Redacted Text Under FOIA Section 40, Personal Information

Email: Redacted Text Under FOIA Section 40, Personal Information

Address: Redacted Text Under FOIA Section 40, Personal Information

BUYER’S ENVIRONMENTAL POLICY

Cabinet Office Environmental Policy Statement available online at: <https://www.gov.uk/government/publications/cabinet-office-environmental-policy-statement>

BUYER’S SECURITY POLICY

**Please refer to** Annex A Security Management - Assurance

SUPPLIER’S AUTHORISED REPRESENTATIVE

**Name:** Redacted Text Under FOIA Section 40, Personal Information

**Role** Redacted Text Under FOIA Section 40, Personal Information

**Email:** Redacted Text Under FOIA Section 40, Personal Information

**Address:** Redacted Text Under FOIA Section 40, Personal Information

PROGRESS REPORT FREQUENCY

In writing on the first Working Day of each calendar month

PROGRESS MEETING FREQUENCY

Weekly verbal updates, as requested

KEY STAFF

Supplier Staff

Redacted Text Under FOIA Section 40, Personal Information

Buyer Staff

Redacted Text Under FOIA Section 40, Personal Information

KEY SUBCONTRACTOR(S)

Redacted Text  Under FOIA Section 43, Commercial Interests

E-AUCTIONS

Not applicable

COMMERCIALLY SENSITIVE INFORMATION

Not applicable

SERVICE CREDITS

Not applicable

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

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

|  |  |  |  |
| --- | --- | --- | --- |
| **For and on behalf of the Supplier:** | | **For and on behalf of the Buyer:** | |
| Signature: | Redacted Text Under FOIA Section 40, Personal Information | Signature: | Redacted Text Under FOIA Section 40, Personal Information |
| Name: | Redacted Text Under FOIA Section 40, Personal Information | Name: | Redacted Text Under FOIA Section 40, Personal Information |
| Role: | Redacted Text Under FOIA Section 40, Personal Information | Role: | Redacted Text Under FOIA Section 40, Personal Information |
| Date: |  | Date: |  |

**Joint Schedule 2 (Variation Form)**

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

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

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

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

|  |  |
| --- | --- |
| Signature |  |

**Joint Schedule 3 (Insurance Requirements)**

# The insurance you need to have

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

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

1.1.2 the Order 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.

# 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.

# 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.

# 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.

# 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.

# Cancelled Insurance

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

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

# Insurance claims

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

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

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

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

**ANNEX: REQUIRED INSURANCES**

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

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

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

| **No.** | **Date** | **Item(s)** | **Duration of Confidentiality** |
| --- | --- | --- | --- |
| 1 | 17/10/22 | Commercial bid submission (including pricing) | To be confirmed |

# Joint Schedule 6 (Key Subcontractors)

1. **Restrictions on certain subcontractors** 
   1. The Supplier is entitled to sub-contract its obligations under the DPS Contract to the Key Subcontractors identified on the Platform.
   2. The Supplier is entitled to sub-contract its obligations under an Order Contract to Key Subcontractors listed on the Platform who are specifically nominated in the Order Form.
   3. Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to the Platform. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to the Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:
      1. the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
      2. the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
      3. the proposed Key Subcontractor employs unfit persons.
   4. The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:
      1. the proposed Key Subcontractor’s name, registered office and company registration number;
      2. the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;
      3. where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm’s-length" terms;
      4. for CCS, the Key Sub-Contract price expressed as a percentage of the total projected DPS Price over the DPS Contract Period;
      5. for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Order Contract Period; and
      6. (where applicable) Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.

RM6126 - Research & Insights DPS

Project Version: v1.0 1

Model Version: v1.1

**Joint Schedule 6 (Key Subcontractors)**

Crown Copyright 2021

* 1. If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:
     1. a copy of the proposed Key Sub-Contract; and
     2. any further information reasonably requested by CCS and/or the Buyer.
  2. The Supplier shall ensure that each new or replacement Key Sub-Contract shall include: 
     1. provisions which will enable the Supplier to discharge its obligations under the Contracts;
     2. a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;
     3. a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;
     4. a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;
     5. obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the DPS Contract in respect of:
        1. the data protection requirements set out in Clause 14 (Data protection);
        2. the FOIA and other access request requirements set out in

Clause 16 (When you can share information);

* + - 1. the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;
      2. the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and
      3. the conduct of audits set out in Clause 6 (Record keeping and reporting);
    1. provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the Buyer can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and
    2. a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

**Joint Schedule 10 (Rectification Plan)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Request for [Revised] Rectification Plan** | | | | | |
| Details of the Default: | [**Guidance:** Explain the Default, with clear schedule and clause references as appropriate] | | | | |
| Deadline for receiving the [Revised] Rectification Plan: | [**add** date (minimum 10 days from request)] | | | | |
| Signed by Buyer : |  | | Date: | |  |
| **Supplier [Revised] Rectification Plan** | | | | | |
| Cause of the Default | [**add** cause] | | | | |
| Anticipated impact assessment: | [**add** impact] | | | | |
| Actual effect of Default: | [**add** effect] | | | | |
| Steps to be taken to rectification: | **Steps** | **Timescale** | | | |
| 1. | [date] | | | |
| 2. | [date] | | | |
| 3. | [date] | | | |
| 4. | [date] | | | |
| […] | [date] | | | |
| Timescale for complete Rectification of Default | [X] Working Days | | | | |
| Steps taken to prevent recurrence of Default | **Steps** | **Timescale** | | | |
| 1. | [date] | | | |
| 2. | [date] | | | |
| 3. | [date] | | | |
| 4. | [date] | | | |
| […] | [date] | | | |
| Signed by the Supplier: |  | Date: | |  | |
| **Review of Rectification Plan** Buyer | | | | | |
| Outcome of review | [Plan Accepted] [Plan Rejected] [Revised Plan Requested] | | | | |
| Reasons for Rejection (if applicable) | [**add** reasons] | | | | |
| Signed by Buyer |  | Date: | |  | |

**Joint Schedule 11 (Processing Data)**

**Definitions**

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

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

**Status of the Controller**

* 1. 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:
     1. “Controller” in respect of the other Party who is “Processor”;
     2. “Processor” in respect of the other Party who is “Controller”;
     3. “Joint Controller” with the other Party;
     4. “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**

* 1. 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.
  2. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
  3. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
     1. a systematic description of the envisaged Processing and the purpose of the Processing;
     2. an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
     3. an assessment of the risks to the rights and freedoms of Data Subjects; and
     4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
  4. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
     1. Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
     2. ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
        1. nature of the data to be protected;
        2. harm that might result from a Personal Data Breach;
        3. state of technological development; and
        4. cost of implementing any measures;
     3. ensure that :
        1. the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));
        2. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
           1. are aware of and comply with the Processor’s duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
           2. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
           3. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
           4. have undergone adequate training in the use, care, protection and handling of Personal Data;
     4. not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
        1. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
        2. the Data Subject has enforceable rights and effective legal remedies;
        3. the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
        4. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
     5. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
  5. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
     1. receives a Data Subject Access Request (or purported Data Subject Access Request);
     2. receives a request to rectify, block or erase any Personal Data;
     3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
     4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
     5. receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
     6. becomes aware of a Personal Data Breach.
  6. The Processor’s obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
  7. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
     1. the Controller with full details and copies of the complaint, communication or request;
     2. such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
     3. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
     4. assistance as requested by the Controller following any Personal Data Breach; and/or
     5. 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.
  8. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
     1. the Controller determines that the Processing is not occasional;
     2. the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
     3. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
  9. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller’s designated auditor.
  10. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
  11. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
      1. notify the Controller in writing of the intended Subprocessor and Processing;
      2. obtain the written consent of the Controller;
      3. enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
      4. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
  12. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
  13. 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).
  14. 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**

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

**Independent Controllers of Personal Data**

* 1. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
  2. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
  3. Where a Party has provided Personal Data to the other Party in accordance with paragraph 8 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
  4. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
  5. The Parties shall only provide Personal Data to each other:
     1. to the extent necessary to perform their respective obligations under the Contract;
     2. 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
     3. where it has recorded it in Annex 1 *(Processing Personal Data).*
  6. 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.
  7. 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.
  8. 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”)**:
     1. 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
     2. where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
        1. promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
        2. provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
  9. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
     1. do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
     2. implement any measures necessary to restore the security of any compromised Personal Data;
     3. work with the other Party to make any required notifications to the Information Commissioner’s Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
     4. 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.
  10. 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).*
  11. 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)*.
  12. 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 27 of this Joint Schedule 11.

## Annex 1 - Processing Personal Data

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

* + - 1. The contact details of the Relevant Authority’s Data Protection Officer are: Redacted Text Under FOIA Section 40, Personal Information
      2. The contact details of the Supplier’s Data Protection Officer are: Redacted Text Under FOIA Section 40, Personal Information
      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 | **The Relevant Authority is Controller and the Supplier is Processor**  The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor |
| Duration of the Processing | Duration of the contract |
| Nature and purposes of the Processing | To design and manage an online survey which will include the following primary questions:   * What are the met and unmet population needs in terms of access to assistive technology? * What is the country’s capacity to meet the identified unmet need? * What is the impact of assistive technology on the people who use it?   This research must comprise an online survey which is as accessible as possible for 5,000-10,000 disabled people, with three components parts:   * A rapid assistive technology assessment survey to measure the need, demand and barriers to accessing assistive technology. * An Assistive Products List survey: which asks disabled people to report which are the most essential assistive products in their daily lives. * Using an assistive technology impact assessment tool to measure the impact of assistive technology on individuals. |
| Type of Personal Data | Contact details, Disability data, Racial/ethnic origins data, Sex/gender data and opinions |
| Categories of Data Subject | Members of the public |
| Plan for return and destruction of the data once the Processing is complete | *All analysis, reports and data collected will be returned/provided to the Disability Unit at the end of this project (excluding personal data – which should be deleted by the supplier first).* |

**Annex 2 - Joint Controller Agreement**

**NOT USED**

**Joint Schedule 12 (Supply Chain Visibility)**

1. **Definitions**

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

|  |  |
| --- | --- |
| **"Contracts Finder"** | the Government’s publishing portal for public sector procurement opportunities; |
| **"SME"** | an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium sized enterprises; |
| **“Supply Chain Information Report Template”** | the document at Annex 1 of this Schedule 12; and |
| **"VCSE"** | a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives. |
|  |  |

1. **Visibility of Sub-Contract Opportunities in the Supply Chain** 
   1. The Supplier shall:
      1. subject to Paragraph 2.3, advertise on Contracts Finder all Sub-Contract opportunities arising from or in connection with the provision of the Deliverables above a minimum threshold of £25,000 that arise during the Contract Period;
      2. within 90 days of awarding a Sub-Contract to a Subcontractor, update the notice on Contract Finder with details of the successful Subcontractor;
      3. monitor the number, type and value of the Sub-Contract opportunities placed on Contracts Finder advertised and awarded in its supply chain during the Contract Period;
      4. provide reports on the information at Paragraph 2.1.3 to the Relevant Authority in the format and frequency as reasonably specified by the Relevant Authority; and
      5. promote Contracts Finder to its suppliers and encourage those organisations to register on Contracts Finder.
   2. Each advert referred to at Paragraph 2.1.1 of this Schedule 12 shall provide a full and detailed description of the Sub-Contract opportunity with each of the mandatory fields being completed on Contracts Finder by the Supplier.
   3. The obligation on the Supplier set out at Paragraph 2.1 shall only apply in respect of Sub-Contract opportunities arising after the Effective Date.
   4. Notwithstanding Paragraph 2.1, the Authority may by giving its prior Approval, agree that a Sub-Contract opportunity is not required to be advertised by the Supplier on Contracts Finder.
2. **Visibility of Supply Chain Spend**
   1. In addition to any other management information requirements set out in the Contract, the Supplier agrees and acknowledges that it shall, at no charge, provide timely, full, accurate and complete SME management information reports (the “SME Management Information Reports”) to the Relevant Authority which incorporates the data described in the Supply Chain Information Report Template which is:
3. the total contract revenue received directly on the Contract;
4. the total value of sub-contracted revenues under the Contract (including revenues for non-SMEs/non-VCSEs); and
5. the total value of sub-contracted revenues to SMEs and VCSEs.
   1. The SME Management Information Reports shall be provided by the Supplier in the correct format as required by the Supply Chain Information Report Template and any guidance issued by the Relevant Authority from time to time. The Supplier agrees that it shall use the Supply Chain Information Report Template to provide the information detailed at Paragraph 3.1(a) –(c) and acknowledges that the template may be changed from time to time (including the data required and/or format) by the Relevant Authority issuing a replacement version. The Relevant Authority agrees to give at least thirty (30) days’ notice in writing of any such change and shall specify the date from which it must be used.
   2. The Supplier further agrees and acknowledges that it may not make any amendment to the Supply Chain Information Report Template without the prior Approval of the Authority.

**Annex 1**

**Supply Chain Information Report template**



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

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

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

**Order Schedule 4 (Order Tender)**

Redacted Text  Under FOIA Section 43, Commercial Interests

**Order Schedule 5 (Pricing Details)**

Redacted Text  Under FOIA Section 43, Commercial Interests

**Order Schedule 7 (Key Supplier Staff)**

* 1. 1.1 The Annex 1 to this Schedule lists the key roles (“**Key Roles**”) and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.
  2. 1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.
  3. 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.
  4. 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. 1.5 The Supplier shall:

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

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

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

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

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

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

**Annex 1- Key Roles**

**Refer to Order Schedule 4 – Order Tender for details**

Order Schedule 9 (Security)

Part A: Short Form Security Requirements

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

|  |  |
| --- | --- |
| "Breach of Security" | 1. the occurrence of:    1. any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or    2. the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, 2. in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2; |
| "Security Management Plan" | 1. the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time; |

1. Complying with security requirements and updates to them
   1. The Buyer and the Supplier recognise that, where specified in DPS Schedule 4 (DPS Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.
   2. The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.
   3. Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.
   4. If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.
   5. Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.
2. Security Standards
   1. The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.
   2. The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:
      1. is in accordance with the Law and this Contract;
      2. as a minimum demonstrates Good Industry Practice;
      3. meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and
      4. where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.
   3. The references to standards, guidance and policies contained or set out in Paragraph 4.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.
   4. In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.
3. Security Management Plan
   1. **Introduction**
      1. The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.
   2. **Content of the Security Management Plan**
      1. The Security Management Plan shall:
         1. comply with the principles of security set out in Paragraph **Error! Reference source not found.** and any other provisions of this Contract relevant to security;
         2. identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
         3. detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer’s Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
         4. be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer’s Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
         5. set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;
         6. set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and
         7. be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.
   3. **Development of the Security Management Plan**
      1. Within twenty (20)Working Days after the Start Date and in accordance with Paragraph 5.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.
      2. If the Security Management Plan submitted to the Buyer in accordance with Paragraph 5.3.1, or any subsequent revision to it in accordance with Paragraph 5.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.
      3. The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 5.3.2. However a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 5.2 shall be deemed to be reasonable.
      4. Approval by the Buyer of the Security Management Plan pursuant to Paragraph 5.3.2 or of any change to the Security Management Plan in accordance with Paragraph 5.4 shall not relieve the Supplier of its obligations under this Schedule.
   4. **Amendment of the Security Management Plan**
      1. The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:
         1. emerging changes in Good Industry Practice;
         2. any change or proposed change to the Deliverables and/or associated processes;
         3. where necessary in accordance with paragraph 2.2, any change to the Security Policy;
         4. any new perceived or changed security threats; and
         5. any reasonable change in requirements requested by the Buyer.
      2. The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:
         1. suggested improvements to the effectiveness of the Security Management Plan;
         2. updates to the risk assessments; and
         3. suggested improvements in measuring the effectiveness of controls.
      3. Subject to Paragraph 5.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 5.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.
      4. The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.
4. Security breach
   1. Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.
   2. Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 6.1, the Supplier shall:
      1. immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:
         1. minimise the extent of actual or potential harm caused by any Breach of Security;
         2. remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;
         3. prevent an equivalent breach in the future exploiting the same cause failure; and
         4. as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.
   3. In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

**Order Schedule 20 (Order Specification)**

1. **PURPOSE**
   1. The Cabinet Office’s Disability Unit publicly committed in the National Disability Strategy (NDS) to undertake a needs and capacity assessment process to improve our understanding of the country’s capacity to finance, procure and provide assistive technology (AT), identifying system inefficiencies and maximising the greatest positive impact on the life outcome for individual AT users.
   2. A more joined-up approach to AT has real potential to help policy makers identify actions to strengthen service delivery to better meet disabled peoples' needs, improving outcomes for them and reducing inefficiencies in our current approach. However, there is a paucity of structured data to develop this approach. Without filling this key evidence gap we cannot push for the required change.
2. **BACKGROUND TO THE CONTRACTING AUTHORITY**
   1. The Contracting Authority is the Cabinet Office, which supports the Prime Minister, and ensures the effective running of government. The Contracting Authority is also the corporate headquarters for the government, in partnership with HM Treasury, and takes the lead in certain critical policy areas. More information about the Contracting Authority can be found on its website at:

<https://www.gov.uk/government/organisations/cabinet-office>

* 1. The Disability Unit is part of the Equalities Hub in the Cabinet Office along with the Race Disparity Unit and Government Equalities Office. The aim of the Disability Unit is to break down barriers faced by disabled people in the UK.

1. **OVERVIEW OF REQUIREMENT**
   1. One of the commitments made in the NDS is to assess the assistive and accessible technology needs of disabled people in England, to establish where these are being met and where improvements can be made.
   2. Technology is often developed without taking into account the needs of disabled people. From streaming services and smartphone apps to AI-powered recruitment and interview tools, the importance of involving disabled people in design processes is clear.
   3. Understanding the met and unmet needs of disabled people, the country’s capacity to meet those needs and understanding the impact of technology on the people who use it will inform the Disability Units additional commitment to develop a new Centre of Assistive and Accessible Technology. Without filling this key evidence gap we cannot push for the required change.
2. **DEFINITIONS**

|  |  |
| --- | --- |
| Expression or Acronym | Definition |
| AT | Assistive Technology |
| Assistive Technology | Assistive Technology - such as wheelchairs, hearing aids, eyeglasses, communication devices, prosthetics, walking aids etc (link to WHO model APL list: <https://www.who.int/phi/implementation/assistive_technology/global_survey-apl/en/>) |
| NDS | National Disability Strategy |
| Disability | Disability is defined in line with the UK census, which asks the question: “Are your day-to-day activities limited because of a health problem or disability which has lasted, or is expected to last, at least 12 months?” |
| Streaming services (para 3.2) | The Big Hack: Scope, 2020 - <https://www.scope.org.uk/big-hack/> |
| Smartphone apps (para 3.2) | Research Institute for Disabled Consumers, Survey of pan-disability panel, 2020 |
| AI-powered recruitment and interview tools (para 3.2) | Review into Bias in Algorithmic Decision Making: Centre for Data Ethics and Innovation, November 2020 |
| The importance of involving disabled consumers in the design process is often emphasised. (para 3.2) | e.g. A review: accessible technology through participatory design: Christian Quintero, July 2020 |

1. **SCOPE OF REQUIREMENT** 
   1. The assistive and accessible technology needs assessment must:
      1. Consider all research questions at 6.2.
      2. Develop and apply a clear set of criteria for testing robustness.
      3. Determine and apply a structure for the final report which is both true to the findings of the survey and easily accessible by non-specialist users.
      4. Identify and document any evidence gaps and/or limitations with the methodology employed.
      5. Structure the report clearly and extract key findings, so policy makers can easily use them to inform policy development and further research.
   2. At a minimum, we expect the outputs to be:
      1. Analysed datasets highlighting key findings.
      2. A written report for the Disability Unit.
      3. Presentation of findings to Disability Unit staff.
2. **THE REQUIREMENT**
   1. The Supplier is required to conduct a needs assessment process to improve our understanding of the country’s capacity to finance, procure and provide assistive technology (AT) identifying system inefficiencies and maximising the greatest positive impact on life outcomes for individual AT users.
   2. To aid the research, it is suggested to minimally address the following primary questions (with secondary research questions included below):
      1. What are the met and unmet population needs in terms of access to assistive technology?
      2. What is the country’s capacity to meet the identified unmet need?
      3. What is the impact of assistive technology on the people who use it?
   3. This research must comprise an online survey which is as accessible as possible for 5,000-10,000 disabled people, with three components parts:
      1. A rapid assistive technology assessment survey to measure the need, demand and barriers to accessing assistive technology.
      2. An Assistive Products List survey: which asks disabled people to report which are the most essential assistive products in their daily lives.
      3. Using an assistive technology impact assessment tool to measure the impact of assistive technology on individuals.
   4. An embargoed report for officials in the Disability Unit will be delivered by the end of the contract:
      1. The report will be set in the context of existing research and evidence about the assistive technology landscape.
      2. The Disability Unit will have the opportunity to review and comment on at least one draft of this before agreeing the final version and approving payment of related invoices. As a minimum, Disability Unit staff would require at least three days to review and return comments on a draft report.
      3. The report must make recommendations for how to progress with an assistive technology capacity assessment, which will evaluate the country’s capacity to finance, regulate, procure and provide ATech efficiently, identifying supply chain and market inefficiencies.
      4. All versions of the report and supporting documentation should be provided to the Disability Unit in Google or Microsoft document formats. If this is not possible an alternative should be agreed in advance with the Disability Unit.
3. **KEY MILESTONES AND DELIVERABLES**
   1. The following Contract milestones/deliverables shall apply:

|  |  |  |
| --- | --- | --- |
| **Milestone/**  **Deliverable** | **Description** | **Timeframe or Delivery Date** |
| 1 | Work commences | By week 1 of contract award |
| 2 | Develop online survey questions in co-production with disabled people. Disability Unit officials given an opportunity to review and agree these. | By week 3 of contract award |
| 3 | Survey launched and open for 2 months. | By week 4 of the contract award |
| 4 | Analysis of data and first draft of final report. | By week 5 of contract award |
| 5 | Final version of report provided and presentation of findings to the Disability Unit | By week 6 of contract award |

1. **MANAGEMENT INFORMATION/REPORTING**
   1. The Supplier will be expected to update and share their work with the Disability Unit at each of the milestones set out in section 7. In addition to this, weekly half-hour meetings are required, to be kept up to date and to allow space for the Supplier to ask questions of the Disability Unit and vice versa. The Supplier should have availability during normal working hours (9am-5.30pm, Mon-Fri) for these meetings, and should have some degree of flexibility around the availability of Disability Unit’s staff.
   2. The Disability Unit will want to engage their network of disability experts and advisors at some or all of these stages, and the Supplier would need to be prepared to have their work scrutinised, validated and challenged by this network.
   3. The Disability Unit will designate a primary point of contact for this work, and the Supplier should update this contact with any significant changes or developments in between regular meetings. Should any questions arise, the Supplier should make contact with the Disability Unit’s primary contact as and when required.
2. **VOLUMES**
   1. This research must comprise an accessible online survey of around 5,000-10,000 disabled people, and will result in a final report which is presented along with findings to the Disability Unit.
3. **CONTINUOUS IMPROVEMENT**
   1. The Supplier will be expected to consider how the required Services could be delivered more effectively in future exercises, learning lessons from the delivery of this particular contract.
   2. The Supplier should present ideas for new and innovative approaches in the final report and during the presentation to Disability Unit officials.
4. **SOCIAL VALUE**
   1. The Supplier will carry out this work in accordance with Social Value requirements linked to the themes of improving wellbeing and creating equal opportunities (see [Procurement Policy Note – Taking Account of Social Value in the Award of Central Government Contracts](https://www.gov.uk/government/publications/procurement-policy-note-0620-taking-account-of-social-value-in-the-award-of-central-government-contracts), September 2020).
   2. The research will be conducted and presented in such a way that policy makers can use it to understand how assistive technology can help disabled people live full and independent lives, participate in society and address issues which are more prevalent amongst the disabled population, such as loneliness or lack of access to local facilities.
   3. Social Value will be assessed along with other service level agreements and performance KPIs (see Section 15 of this document).
5. **QUALITY**
   1. The online surveys should be made to be as accessible to as wide a range of disabled people, as possible.
   2. The AT needs assessment should be completed to a high academic standard.
   3. The final output should be completed to a high standard in terms of the accessibility and ease of use for a wide range of non-specialist users.
6. **PRICE**
   1. The maximum budget for this work is Redacted Text Under FOIA Section 43, Commercial Interests. In providing a fixed price, the Supplier should make it clear how many person days will be devoted to completing this work, and provide a breakdown of price for each milestone. If applicable, this should be separated out between different individuals/roles, making clear the skill/experience level and cost of each individual.
   2. Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule including VAT and including all other expenses relating to Contract delivery.
   3. Invoices for the work should be submitted within 24 hours of each milestone being met. Please Section 17 of this document for full details of Payments and Invoicing.
7. **STAFF AND CUSTOMER SERVICE**
   1. The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
   2. The Supplier’s staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
   3. The Supplier shall ensure that staff understand the Contracting Authority’s vision and objectives and will provide excellent customer service to the Contracting Authority throughout the duration of the Contract.
8. **SERVICE LEVELS AND PERFORMANCE**
   1. The Contracting Authority will measure the quality of the Supplier’s delivery against each of the following service areas:

|  |  |  |
| --- | --- | --- |
| KPI/SLA | Service Area | KPI/SLA description |
| 1 | Delivery timescales | All milestones outlined in Section 7 above are met within 24 hours of the target date. |
| 2 | Delivery timescales | Final project including report and presentation to Disability Unit officials is delivered within the 4 month timeframe. |
| 3 | Survey outcomes | Ensure policy makers understand how they can apply the findings to achieve the objectives set out in the Purpose section above (1), including its application to the work of the Centre for Assistive and Accessible Technology (see 3.3) |
| 4 | Social Value | The Supplier maintains a focus on how AT adds social value and explains this to policy makers using their findings (see 11). |

* 1. The Disability unit will have regular catch ups with the Supplier to monitor delivery.
  2. Due to the length of this contract there are no exit strategies to be applied.

1. **SECURITY AND CONFIDENTIALITY REQUIREMENTS**
   1. The Supplier will not be required to undertake security vetting.
   2. The Supplier will largely be working with information already accessible to them in the public domain. Any documents or information shared with the Supplier by Disability Unit should remain confidential and not be shared further.
2. **PAYMENT AND INVOICING** 
   1. Invoices should be submitted upon confirmation from the Contracting Authority that delivery of the milestones has been met. The Contracting Authority will provide the Supplier with a Purchase Order Number to enable invoicing.
   2. Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.
   3. Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs, so that it can be approved by Disability Unit officials.
   4. Invoices should be submitted to: Redacted Text Under FOIA Section 40, Personal Information
   5. A copy of each invoice should also be sent to Redacted Text Under FOIA Section 40, Personal Informatio

1. **CONTRACT MANAGEMENT** 
   1. The contract will be managed through the processes set out in Section 8.
   2. All meetings shall be conducted remotely via Google Hangouts/Zoom, so the Supplier shall not incur any travel expenses to attend these meetings.
2. **LOCATION**
   1. The services will be carried out remotely at the Supplier’s chosen location.

Annex A Security Schedule

SECURITY MANAGEMENT - ASSURANCE

1. Definitions

In this Schedule:

|  |  |
| --- | --- |
| **“Anti-Malicious Software”** | means software that scans for and identifies possible Malicious Software in the IT Environment; |
| **“Breach of Security”** | 1. an event that results, or could result, in: 2. any unauthorised access to or use of the Authority Data, the Services and/or the Information Management System; and/or 3. the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Authority and/or the Supplier in connection with this Call-Off Contract; |
| **“Certification Requirements”** | means the information security requirements set out in Paragraph 5; |
| **“CHECK Service Provider”** | means a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the IT Health Check services required by Paragraph 6.1; |
| **“CREST Service Provider”** | means a company with a SOC Accreditation from CREST International; |
| **“Higher Risk Sub-contractor”** | means a Sub-contractor that Processes Authority Data, where that data includes either:   1. the Personal Data of 1,000 or more individuals in aggregate during the period between the first Operational Service Commencement Date and the date on which this Agreement terminates in accordance with Clause 4.1(b); or 2. Special Category Personal Data; |
| **“Cyber Essentials”** | means the Cyber Essentials certificate issued under the Cyber Essentials Scheme; |
| **“Cyber Essentials Plus”** | means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme; |
| **“Cyber Essentials Scheme”** | means the Cyber Essentials scheme operated by the National Cyber Security Centre; |
| **“Incident Management Process”** | means the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Authority Data, the Authority, the Services and/or users of the Services and which shall be shall be prepared by the Supplier in accordance with Paragraph 3 using the template set out in Annex 3; |
| **“Information Assurance Assessment”** | means the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Paragraph 3 in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using the template set out in Annex 3; |
| **“Information Management System”** | means   1. those parts of the Supplier System, and those of the Sites, that the Supplier or its Sub-contractors will use to provide the parts of the Services that require Processing Authority Data; and 2. the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); |
| **“Information Security Approval Statement”** | means a notice issued by the Authority which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that:   1. the Authority is satisfied that the identified risks have been adequately and appropriately addressed; 2. the Authority has accepted the residual risks; and 3. the Supplier may use the Information Management System to Process Authority Data; |
| **“IT Health Check”** | has the meaning given in Paragraph 6.1; |
| **“Medium Risk Sub-contractor”** | means a Sub-contractor that Processes Authority Data, where that data   1. includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the first Operational Service Commencement Date and the date on which this Agreement terminates in accordance with Clause 4.1(b); and 2. does not include Special Category Personal Data; |
| **“Personal Data Processing Statement”** | means a document setting out:   1. the types of Personal Data which the Supplier and/or its Sub-contractors Processes or will Process under this Agreement; 2. the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors Processes or will Process under this Agreement; 3. the nature and purpose of such Processing; 4. the locations at which the Supplier and/or its Sub-contractors Process Personal Data under this Agreement; and 5. the Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data Processed under this Agreement against a Breach of Security (insofar as that Breach of Security relates to data) or a Personal Data Breach; |
| **“Process”** | means any operation which is performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; |
| **“Required Changes Register”** | mean the register within the Security Management Plan which is to be maintained and updated by the Supplier and which shall record each of the changes that the Supplier shall make to the Information Management System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in Paragraph 4.2 together with the date by which such change shall be implemented and the date on which such change was implemented; |
| **“Risk Register”** | is the risk register within the Information Assurance Assessment which is to be prepared and submitted to the Authority for approval in accordance with Paragraph 3; |
| **“Security Management Plan”** | means the document prepared by the Supplier using the template in Annex 3, comprising:   1. the Information Assurance Assessment; 2. the Personal Data Processing Statement; 3. the Required Changes Register; and 4. the Incident Management Process; |
| **Special Category Personal Data** | means the categories of Personal Data set out in article 9(1) of the GDPR; |

1. Introduction
   1. This Schedule sets out:
      1. the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Call-Off Contract to ensure the security of the Authority Data and the Information Management System;
      2. the Certification Requirements applicable to the Supplier and each of those Sub-contractors which Processes Authority Data;
      3. The security requirements in Annex 1, with which the Supplier must comply;
      4. the tests which the Supplier shall conduct on the Information Management System during the Term;
      5. the Supplier's obligations to:
         1. return or destroy Authority Data on the expiry or earlier termination of this Agreement; and
         2. prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in Paragraph 8; and
         3. report Breaches of Security to the Authority.
2. Principles of Security
   1. The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:
      1. the Sites;
      2. the IT Environment;
      3. the Information Management System; and
      4. the Services.
   2. Notwithstanding the involvement of the Authority in assessing the arrangements which the Supplier implements to ensure the security of the Authority Data and the Information Management System, the Supplier shall be, and shall remain, responsible for:
      1. the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors; and
      2. the security of the Information Management System.
   3. The Supplier shall:
      1. comply with the security requirements in Annex 1; and
      2. ensure that each Sub-contractor that Processes Authority Data complies with the Sub-contractor Security Requirements.
   4. The Supplier shall provide the Authority with access Supplier Personnel responsible for information assurance to facilitate the Authority's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.
3. Information Security Approval Statement
   1. The Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Schedule, including any requirements imposed on Sub-contractors by Annex 2, from the first Operational Services Commencement Date.
   2. The Supplier may not use the Information Management System to Process Authority Data unless and until:
      1. the Supplier has procured the conduct of an IT Health Check of the Supplier System by a CHECK Service Provider or a CREST Service Provider in accordance with Paragraph 6.1; and
      2. the Authority has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 3.
   3. The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule 9 and the Agreement in order to ensure the security of the Authority Data and the Information Management System.
   4. The Supplier shall prepare and submit to the Authority within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which comprises:
      1. an Information Assurance Assessment;
      2. the Required Changes Register;
      3. the Personal Data Processing Statement; and
      4. the Incident Management Process.
   5. The Authority shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within 20 Working Days of receipt and shall either issue the Supplier with:
      1. an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Authority Data; or
      2. a rejection notice, which shall set out the Authority's reasons for rejecting the Security Management Plan.
   6. If the Authority rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Authority's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Authority for review within 10 Working Days or such other timescale as agreed with the Authority.
   7. The Authority may require, and the Supplier shall provide the Authority and its authorised representatives with:
      1. access to the Supplier Personnel;
      2. access to the Information Management System to audit the Supplier and its Sub-contractors’ compliance with this Agreement; and
      3. such other information and/or documentation that the Authority or its authorised representatives may reasonably require,

to assist the Authority to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Authority Data and the Information Management System are consistent with the representations in the Security Management Plan. The Supplier shall provide the access required by the Authority in accordance with this Paragraph within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Authority with the access that it requires within 24 hours of receipt of such request.

1. Compliance Reviews
   1. The Supplier shall regularly review and update the Security Management Plan, and provide such to the Authority, at least once each year and as required by this Paragraph.
   2. The Supplier shall notify the Authority within 2 Working Days after becoming aware of:
      1. a significant change to the components or architecture of the Information Management System;
      2. a new risk to the components or architecture of the Information Management System;
      3. a vulnerability to the components or architecture of the Service which is classified 'Medium', 'High', 'Critical' or 'Important' in accordance with the classification methodology set out in Paragraph 9.2 of Annex 1 to this Schedule;
      4. a change in the threat profile;
      5. a significant change to any risk component;
      6. a significant change in the quantity of Personal Data held within the Service;
      7. a proposal to change any of the Sites from which any part of the Services are provided; and/or
      8. an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.
   3. Within 10 Working Days of such notifying the Authority or such other timescale as may be agreed with the Authority, the Supplier shall make the necessary changes to the Required Changes Register and submit the updated Required Changes Register the Authority for review and approval.
   4. Where the Supplier is required to implement a change, including any change to the Information Management System, the Supplier shall effect such change at its own cost and expense.
2. Certification Requirements
   1. The Supplier shall be certified as compliant with:
      1. ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and
      2. Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier shall be permitted to receive, store or Process Authority Data.

* 1. The Supplier shall ensure that each Higher Risk Sub-contractor is certified as compliant with either:
     1. ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; or
     2. Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Higher-Risk Sub-contractor shall be permitted to receive, store or Process Authority Data.

* 1. The Supplier shall ensure that each Medium Risk Sub-contractor is certified compliant with Cyber Essentials.
  2. The Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:
     1. securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and
     2. are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Authority.
  3. The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph before the Supplier or the relevant Sub-contractor (as applicable) may carry out the secure destruction of any Authority Data.
  4. The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-contractor shall:
     1. immediately ceases using the Authority Data; and
     2. procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with the requirements set out in this Paragraph.
     3. The Authority may agree to exempt, in whole or part, the Supplier or any Sub-contractor from the requirements of this Paragraph 5. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

1. Security Testing
   1. The Supplier shall, at its own cost and expense procure and conduct:
      1. testing of the Information Management System by a CHECK Service Provider or a CREST Service Provider (“**IT Health Check**”); and
      2. such other security tests as may be required by the Authority,
   2. The Supplier shall complete all of the above security tests before the Supplier submits the Security Management Plan to the Authority for review in accordance with Paragraph 3; and it shall repeat the IT Health Check not less than once every 12 months during the Term and submit the results of each such test to the Authority for review in accordance with this Paragraph.
   3. In relation to each IT Health Check, the Supplier shall:
      1. agree with the Authority the aim and scope of the IT Health Check;
      2. promptly, and no later than 10 working days, following the receipt of each IT Health Check report, provide the Authority with a copy of the full report;
      3. in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall: spef
         1. prepare a remedial plan for approval by the Authority (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:
            1. how the vulnerability will be remedied;
            2. unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied, which must be:

within three months of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “medium”;

within one month of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “high”; and

within 10 Working Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “critical”;

* + - * 1. the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;
      1. comply with the Vulnerability Correction Plan; and
      2. conduct such further tests on the Service as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.
  1. The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Authority.
  2. If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique that has the potential to affect the security of the Information Management System, the Supplier shall within 2 Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Authority with a copy of the test report and:
     1. propose interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available; and
     2. where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Supplier System) within the timescales set out in the test report or such other timescales as may be agreed with the Authority.
  3. The Supplier shall conduct such further tests of the Supplier System as may be required by the Authority from time to time to demonstrate compliance with its obligations set out this Schedule and the Call-Off Contract.
  4. The Supplier shall notify the Authority immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Annex 1 to this Schedule.

1. Security Monitoring and Reporting
   1. The Supplier shall:
      1. monitor the delivery of assurance activities;
      2. maintain and update the Security Management Plan in accordance with Paragraph 4;
      3. agree a document which presents the residual security risks to inform the Authority’s decision to give approval to the Supplier to Process, store and transit the Authority Data;
      4. monitor security risk impacting upon the operation of the Service;
      5. report Breaches of Security in accordance with the approved Incident Management Process;
      6. agree with the Authority the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Authority within 20 Working Days of Effective Date.
2. Malicious Software
   1. The Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Information Management System which may Process Authority Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.
   2. If Malicious Software is found, the parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.
   3. Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 8.2 shall be borne by the parties as follows:
      1. by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier or the Authority Data (whilst the Authority 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 Authority when provided to the Supplier; and
      2. by the Authority, in any other circumstance.
3. Breach of Security
   1. If either party becomes aware of a Breach of Security it shall notify the other in accordance with the Incident Management Process.
   2. The Incident Management Process shall, as a minimum, require the Supplier to do the following upon it becoming aware of a Breach of Security or attempted Breach of Security:
      1. Immediately take all reasonable steps necessary to:
         1. minimise the extent of actual or potential harm caused by such Breach of Security;
         2. remedy such Breach of Security to the extent possible;
         3. apply a tested mitigation against any such Breach of Security; and
         4. prevent a further Breach of Security in the future which exploits the same root cause failure;
      2. as soon as reasonably practicable and, in any event, within 2 Working Days, following the Breach of Security or attempted Breach of Security, provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.
   3. In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Sub-contractors and/or all or any part of the Information Management System with this Call-Off Contract, then such remedial action shall be completed at no additional cost to the Authority.

**Annex 1: Security Requirements**

1. Security Classification of Information

If the provision of the Services requires the Supplier to Process Authority Data which is classified as OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

1. End User Devices
   1. The Supplier must manage, and must ensure that all Key Sub-contractors manage, all End-user Devices on which Authority Data is stored or processed in accordance the following requirements:
      1. the operating system and any applications that store, process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
      2. users must authenticate before gaining access;
      3. all Authority Data must be encrypted using a encryption tool agreed to by the Authority;
      4. the End-under Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
      5. the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data;
      6. the Supplier or Key Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device; and
      7. all End-user Devices are within in the scope of any current Cyber Essentials Plus certificate  held by the Supplier, or any ISO/IEC 27001:2013 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.
   2. The Supplier must comply, and ensure that all Key Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.
   3. Where there any conflict between the requirements of this Schedule (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.
2. Encryption
   1. The Supplier must ensure, and must ensure that all Key Sub-contractors ensure, that Authority Data is encrypted;
      1. when stored at any time when no operation is being performed on it; and;
      2. when transmitted.
   2. Where the Supplier, or a Key Sub-contractor, cannot encrypt Authority Data as required by Paragraph 3.1of this Annex 1, the Supplier must:
      1. immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
      2. provide details of the protective measures the Supplier or Key Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption;
      3. provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.
      4. once the Authority and the Supplier reach agreement, update the Security Management Plan to include:
         1. the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and
         2. the protective measure that the Supplier and/or Key Sub-contractor will put in place in respect of the unencrypted Authority Data.
3. Personnel Security
   1. 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 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.
   2. The Authority and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Authority Data or data which, if it were Authority Data, would be classified as OFFICIAL-SENSITIVE.
   3. The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.
   4. The Supplier shall ensure that Supplier Personnel are only granted such access to Authority Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.
   5. The Supplier shall ensure that Supplier Personnel who no longer require access to the Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Authority Data revoked within 1 Working Day.
   6. The Supplier shall ensure that Supplier Staff that have access to the Sites, the IT Environment or the Authority Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the IT Environment or the Authority Data.
   7. The Supplier shall ensure that the training provided to Supplier Staff under paragraph 4.6 includes training on the identification and reporting fraudulent communications intended to induce individuals to disclose Personal Data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Sites, the IT Environment or the Authority Data (“phishing”).
4. Identity, Authentication and Access Control
   1. The Supplier shall operate an access control regime to ensure:
      1. all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and
      2. all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.
   2. The Supplier shall apply the ‘principle of least privilege’ when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require.
   3. The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Authority on request.
5. Data Destruction or Deletion

The Supplier shall:

* 1. prior to securely sanitising any Authority Data or when requested the Supplier shall provide the Government with all Authority Data in an agreed open format;
  2. have documented processes to ensure the availability of Authority Data in the event of the Supplier ceasing to trade;
  3. securely erase in a manner agreed with the Authority any or all Authority Data held by the Supplier when requested to do so by the Authority;
  4. securely destroy in a manner agreed with the Authority all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Call-Off Contract and, in the absence of any such requirements, as agreed by the Authority; and
  5. implement processes which address the CPNI and NCSC guidance on secure sanitisation.

1. Audit and Protective Monitoring
   1. The Supplier shall collect audit records which relate to security events in the Information Management System 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 Information Management System, 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 Data.
   2. The Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the Information Management System.
   3. The retention periods for audit records and event logs must be agreed with the Authority and documented in the Security Management Plan.
2. Location of Authority Data

The Supplier shall not and shall procure that none of its Sub-contractors Process Authority Data outside the United Kingdom or EEA without the prior written consent of the Authority, which may be subject to conditions.

1. Vulnerabilities and Corrective Action
   1. The Authority and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Authority Data.
   2. The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as ‘Critical’, ‘Important’ and ‘Other’ by aligning these categories to the vulnerability scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:
      1. the ‘National Vulnerability Database’ ‘Vulnerability Severity Ratings’: ‘High’, ‘Medium’ and ‘Low’ respectively (these in turn are aligned to CVSS scores as set out by NIST at http://nvd.nist.gov/cvss.cfm); and
      2. Microsoft’s ‘Security Bulletin Severity Rating System’ ratings ‘Critical’, ‘Important’, and the two remaining levels (‘Moderate’ and ‘Low’) respectively.
   3. Subject to Paragraph 9.4, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:
      1. 7 days after the public release of patches for those vulnerabilities categorised as ‘Critical’;
      2. 30 days after the public release of patches for those vulnerabilities categorised as ‘Important’; and
      3. 60 days after the public release of patches for those vulnerabilities categorised as ‘Other’.
   4. The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph 9.3 shall be extended where:
      1. the Supplier can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 9.3 if the vulnerability becomes exploitable within the context of the Services;
      2. the application of a ‘Critical’ or ‘Important’ security patch adversely affects the Supplier’s ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or
      3. the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan.
   5. The Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Authority in writing. All COTS Software should be no more than N-1 versions behind the latest software release.
2. Secure Architecture
   1. The Supplier shall design the Information Management System in accordance with:
      1. the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main>;
      2. the NCSC "Bulk Data Principles", a copy of which can be found at https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main; and
      3. the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:
         1. "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;
         2. "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;
         3. "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;
         4. "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;
         5. "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;
         6. "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;
         7. "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;
         8. "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;
         9. "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Service;
         10. "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;
         11. "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;
         12. "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;
         13. "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors; and
         14. "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

**Annex 2: Security Requirements for Sub-contractors**

1. Application of Annex
   1. This Annex applies to all Sub-contractors that Process Authority Data.
   2. The Supplier must:
      1. ensure that those Sub-contractors comply with the provisions of this Annex;
      2. keep sufficient records to demonstrate that compliance to the Authority; and
      3. ensure that its Implementation Plan includes Deliverable Items, Milestones and Milestone Dates that relate to the design, implementation and management of any systems used by Sub-contractors to Process Authority Data.
2. Designing and managing secure solutions
   1. The Sub-contractor shall implement their solution(s) to mitigate the security risks in accordance with the NCSC’s Cyber Security Design Principles <https://www.ncsc.gov.uk/collection/cyber-security-design-principles>.
   2. The Sub-contractor must assess their systems against the NCSC Cloud Security Principles: [https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles](https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles%20) at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Authority on the Authority’s request.
3. Data Processing, Storage, Management and Destruction
   1. The Sub-contractor must not Process any Authority Data outside the United Kingdom. The Authority may permit the Sub-contractor to Process Authority Data outside the United Kingdom and may impose conditions on that permission, with which the Sub-contractor must comply. Any permission must be in writing to be effective.
   2. The Sub-contractor must securely erase any or all Authority Data held by the Sub-contractor when requested to do so by the Authority; and securely destroy all media that has held Authority Data at the end of life of that media in accordance with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard, or an alternative agreed in writing by the Authority.
4. Personnel Security
   1. The Sub-contractor must perform appropriate checks on their staff before they may participate in the provision and or management of the Services. Those checks must include all pre-employment checks required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The HMG Baseline Personnel Security Standard is at https://www.gov.uk/government/publications/government-baseline-personnel-security-standard.
   2. The Sub-contractor must, if the Authority requires, at any time, ensure that one or more of the Sub-contractor’s staff obtains Security Check clearance in order to Process Authority Data containing Personal Data above certain volumes specified by the Authority, or containing Special Category Personal Data.
   3. Any Sub-contractor staff who will, when performing the Services, have access to a person under the age of 18 years must undergo DBS checks
5. End User Devices
   1. The Sub-contractor shall ensure that any Authority Data stored (for any period of time) on a mobile, removable or physically uncontrolled device is encrypted. The Sub-contractor must follow the Information Commissioner’s Office guidance on implementing encryption, which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/.
   2. The Supplier shall ensure that any device used to Process Authority Data meets all the security requirements set out in the NCSC End User Devices Platform Security Guidance, which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security>.
6. Networking

The Supplier shall ensure that any Authority 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.

1. Patching and Vulnerability Scanning
   1. The Sub-contractor must proactively monitor supplier vulnerability websites and ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the NCSC Cloud Security Principles.
2. Third Party Sub-contractors
   1. The Sub-contractor must not transmit or disseminate the Authority Data to any other person unless specifically authorised by the Authority. Such authorisation must be in writing to be effective and may be subject to conditions.
   2. The Sub-contractor must not, when performing any part of the Services, use any software to Process the Authority Data where the licence terms of that software purport to grant the licensor rights to Progress the Authority Data greater than those rights strictly necessary for the use of the software.

**Annex 3: Security Management Plan Template**

****