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

**Schedules)**

**Order Form**

|  |  |
| --- | --- |
| ORDER REFERENCE: | **SR1312500988** |
| THE BUYER: | HM Revenue & Customs |
| BUYER ADDRESS | HM Revenue & Customs (HMRC) xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  xxxxxxxxxxxxxxxx |
| THE SUPPLIER: | AMR Cyber Security Ltd |
| SUPPLIER ADDRESS: | xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxx xxxxxxxxxxxxxx |
| REGISTRATION NUMBER: |  |
| DUNS NUMBER: | xxxxxxxxx |

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated **15/01/2024**

It’s issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Security Services.

DPS FILTER CATEGORY(IES):

Not applicable

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) RM3764iii
3. The following Schedules in equal order of precedence:

* + Joint Schedules for RM3764iii

o Joint Schedule 2 (Variation Form)

o Joint Schedule 3 (Insurance Requirements)

* + - Joint Schedule 7 (Financial Difficulties)
    - Joint Schedule 8 (Guarantee)
    - Joint Schedule 10 (Rectification Plan)
    - Joint Schedule 11 (Processing Data)

* + Order Schedules for RM3764iii
    - Order Schedule 1 (Transparency Reports)
    - Order Schedule 2 (Staff Transfer)
    - Order Schedule 4 (Order Tender)
    - Order Schedule 5 (Pricing Details)
    - Order Schedule 6 (ICT Services)
    - Order Schedule 7 (Key Supplier Staff )
    - Order Schedule 8 (Business Continuity and Disaster Recovery)
    - Order Schedule 9 (Security)
    - Order Schedule 10 (Exit Management)
    - Order Schedule 13 (Implementation Plan and Testing)
    - Order Schedule 20 (Order Specification)

1. CCS Core Terms (DPS version)
2. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii
3. Annexes A & B to Order Schedule 6
4. ‘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

**HMRC Mandatory Additional Terms**

ORDER START DATE:

ORDER EXPIRY DATE: xx/xx/2023 20 days after signature

ORDER INITIAL PERIOD: 24 Months

ORDER OPTIONAL EXTENSION 12 months + 12 months

DELIVERABLES

**Option B** - 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

xxxxxxxxx

ORDER CHARGES

Price is zero-committed spend contract up to the value of £3,000,000

REIMBURSABLE EXPENSES

Recoverable as stated in the DPS Contract

PAYMENT METHOD

Price is zero-committed spend contract up to the value of £3,000,000

Invoices and payments to go through HMRC SAP Ariba

BUYER’S INVOICE ADDRESS:

Invoices will be sent via SAP Ariba system

**PLEASE NOTE:**

All invoices must include:

* the Purchase Order number;
* total value excluding Value Added Tax (VAT);
* the VAT percentage;
* the total value including VAT;
* a contact name and telephone number of an appropriate individual in the Supplier's finance department in the event of administrative queries; and the banking details for payment to the Supplier via electronic transfer of funds (name and address of bank, sort code, account name and number).
* CSTS Reference for each item of work

BUYER’S AUTHORISED REPRESENTATIVE

xxxxxxxxx

xxxxxxxxxxxxxxxx

xxxxxxxxxxx

xxxxxxxxx xxxxxxxxx

xxxxxxxxx xxxxxxxxx

xxxxxxxxx

BUYER’S ENVIRONMENTAL POLICY

N/A

BUYER’S SECURITY POLICY

**Please see Appendix A – HMRC Mandatory Additional Clauses**

SUPPLIER’S AUTHORISED REPRESENTATIVE

xxxxxxxxx

xxxxxxx

xxxxxxxxx xxxxxxxxx

xxxxxxxxx xxxxxxxxx xxxxxxxxx xxxxxxxxx xxxxxxxxx

SUPPLIER’S CONTRACT MANAGER

xxxxxxxxxxxxx

xxxxxxxxx

xxxxxxxxx xxxxxxxxx

xxxxxxxxx xxxxxxxxx xxxxxxxxx

PROGRESS REPORT FREQUENCY

Third week of each month– to include Social Value. (when relevant)

PROGRESS MEETING FREQUENCY

Third week of each month– to include Social Value. (when relevant)

KEY STAFF

xxxxxxxxx

xxxxxxx

xxxxxxxxx xxxxxxxxx

xxxxxxxxx xxxxxxxxx xxxxxxxxx xxxxxxxxx xxxxxxxxx

xxxxxxxxxxxxx

xxxxxxxxx

xxxxxxxxx xxxxxxxxx

xxxxxxxxx xxxxxxxxx xxxxxxxxx

xxxxxxxxxxxxxxx

xxxxxxxxxxx

xxxxxxxxx xxxxxxxxx

xxxxxxxxx xxxxxxxxx xxxxxxxxx

KEY SUBCONTRACTOR(S)

xxxxxxx xxxxxxxxx

COMMERCIALLY SENSITIVE INFORMATION

Not applicable

SERVICE CREDITS

Service credits have been provided across a sample of KPIs to ensure that the contact is being delivered in accordance with KPIs and to demonstrate collaborative good intention from the supplier.

All the KPIs/SLA.s called out in Schedule 16 of this contract apply.

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: | xxxxxxxxx | Signature: | xxxxxxxxx |
| Name: | xxxxxxxxx | Name: | xxxxxxxxx |
| Role: | xxxxxxxxx | Role: | xxxxxxxxx |
| Date: | xxxxxxxxx | Date: | xxxxxxxxx |

**Order Schedule 4 (Order Tender) - REDACTED**

Order Schedule 9 (Security)

Part B: Long 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. means the occurrence of:    1. any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or    2. the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, 2. in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d; |
| "ISMS" | 1. the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and |
| "Security Tests" | 1. tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security. |

1. Security Requirements
   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 Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.
   3. The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:
      1. HMRC – Gareth Perry
   4. The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.
   5. Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.
   6. The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.
   7. The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.
   8. The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer’s security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.
2. Information Security Management System (ISMS)
   1. The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.
   2. The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.
   3. The Buyer acknowledges that;
      1. If the Buyer has not stipulated during an Order Procedure that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier’s estate; and
      2. Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer’s Approval.
   4. The ISMS shall:
      1. if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer’s Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;
      2. meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;
      3. at all times provide a level of security which:
         1. is in accordance with the Law and this Contract;
         2. complies with the Baseline Security Requirements;
         3. as a minimum demonstrates Good Industry Practice;
         4. where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;
         5. complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4)(<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>)
         6. takes account of guidance issued by the Centre for Protection of National Infrastructure <https://www.cpni.gov.uk/>
         7. complies with HMG Information Assurance Maturity Model and Assurance Framework (<https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm>);
         8. meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;
         9. addresses issues of incompatibility with the Supplier’s own organisational security policies; and
         10. complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;
      4. document the security incident management processes and incident response plans;
      5. document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and
      6. be certified by (or by a person with the direct delegated authority of) a Supplier’s main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).
   5. Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.
   6. In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.
   7. If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.
   8. Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.
3. Security Management Plan
   1. Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4.3 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.
   2. The Security Management Plan shall:
      1. be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);
      2. comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;
      3. identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;
      4. detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer’s Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;
      5. unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer’s Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
      6. set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);
      7. demonstrate that the Supplier’s approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, ‘platform as a service’ offering from the G-Cloud catalogue);
      8. set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;
      9. set out the scope of the Buyer System that is under the control of the Supplier;
      10. be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and
      11. be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.
   3. If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.
   4. Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.
4. Amendment of the ISMS and Security Management Plan
   1. The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:
      1. emerging changes in Good Industry Practice;
      2. any change or proposed change to the Supplier System, the Deliverables and/or associated processes;
      3. any new perceived or changed security threats;
      4. where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;
      5. any new perceived or changed security threats; and
      6. any reasonable change in requirement 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 amend the ISMS and 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 ISMS;
      2. updates to the risk assessments;
      3. proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and
      4. suggested improvements in measuring the effectiveness of controls.
   3. Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex nnex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.
   4. The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.
5. Security Testing
   1. The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier’s ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.
   2. The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.
   3. Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer’s test adversely affects the Supplier’s ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer’s test.
   4. Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.
   5. If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.
6. Complying with the ISMS
   1. The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.
   2. If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.
   3. If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.
7. Security Breach
   1. Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.
   2. Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:
      1. immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:
         1. minimise the extent of actual or potential harm caused by any Breach of Security;
         2. remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier’s control;
         3. apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier’s ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;
         4. prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and
         5. supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer’s request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and
         6. as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.
   3. In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.
8. Vulnerabilities and fixing them
   1. The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer’s information.
   2. The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as ‘Critical’, ‘Important’ and ‘Other’ by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:
      1. the ‘National Vulnerability Database’ ‘Vulnerability Severity Ratings’: ‘High’, ‘Medium’ and ‘Low’ respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and
      2. Microsoft’s ‘Security Bulletin Severity Rating System’ ratings ‘Critical’, ‘Important’, and the two remaining levels (‘Moderate’ and ‘Low’) respectively.
   3. The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as ‘Critical’ within 14 days of release, ‘Important’ within 30 days of release and all ‘Other’ within 60 Working Days of release, except where:
      1. the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;
      2. the application of a ‘Critical’ or ‘Important’ security patch adversely affects the Supplier’s ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or
      3. the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.
   4. The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the ‘n-1 version’) throughout the Term unless:
      1. where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or
      2. is agreed with the Buyer in writing.
   5. The Supplier shall:
      1. implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;
      2. ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
      3. ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;
      4. pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.4.5;
      5. from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;
      6. propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;
      7. remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and
      8. inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.
   6. If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.
   7. A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:

Baseline security requirements

1. Handling Classified information
   1. The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.
2. End user devices
   1. When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").
   2. Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a ‘known good’ state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (<https://www.ncsc.gov.uk/guidance/end-user-device-security)>. Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Buyer.
3. Data Processing, Storage, Management and Destruction
   1. The Supplier and Buyer recognise the need for the Buyer’s information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.
   2. The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).
   3. The Supplier shall:
      1. provide the Buyer with all Government Data on demand in an agreed open format;
      2. have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;
      3. securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and
      4. securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.
4. Ensuring secure communications
   1. The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA.
   2. The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.
5. Security by design
   1. The Supplier shall apply the ‘principle of least privilege’ (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.
   2. When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (<https://www.ncsc.gov.uk/articles/cesg-certification-ia-professionals-and-guidance-certification-ia-professionals-documents>) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).
6. Security of Supplier Staff
   1. Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.
   2. The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as ‘SC’) including system administrators with privileged access to IT systems which store or process Government Data.
   3. The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.
   4. All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.
   5. Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.
7. Restricting and monitoring access
   1. The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the ‘principle of least privilege’, users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.
8. Audit
   1. The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:
      1. Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.
      2. Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.
   2. The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.
   3. The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B – Annex 2 – Redacted

**Order Schedule 20 (Order Specification)** - **Redacted**

**Appendix A – HMRC Mandatory Additional Clauses**

Version control: v1.2, January 2022



Appendix A

AUTHORITY’S MANDATORY TERMS

1. For the avoidance of doubt, references to ‘the Agreement’ mean the attached Call-Off Contract between the Supplier and the Authority. References to ‘the Authority’ mean ‘the Buyer’ (the Commissioners for Her Majesty’s Revenue and Customs).
2. The Agreement incorporates the Authority’s mandatory terms set out in this Schedule.
3. In case of any ambiguity or conflict, the Authority’s mandatory terms in this Schedule will supersede any other terms in the Agreement.
4. For the avoidance of doubt, the relevant definitions for the purposes of the defined terms set out in the Authority’s mandatory terms in this Schedule are the definitions set out at Clause 1 of this Schedule.

# 1. Definitions

“Affiliate” in relation to a body corporate, any other entity which directly or

indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;

“Authority Data” (a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:

1. supplied to the Supplier by or on behalf of the Authority; and/or
2. which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or

(b) any Personal Data for which the Authority is the Controller, or any data derived from such Personal Data which has had any designatory data identifiers removed so that an individual cannot be identified;

“Charges” the charges for the Services as specified in as per order form and contract.

“Connected means, in relation to a company, entity or other person, the Affiliates of

Company” that company, entity or other person or any other person associated with such company, entity or other person;

|  |  |
| --- | --- |
| “Control” | the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly; |
| “Controller”,  “Processor”, “Data  Subject”, | take the meaning given in the UK GDPR; |
| “Data Protection  Legislation” | 1. "the data protection legislation" as defined in section 3(9) of the Data Protection Act 2018; and; 2. all applicable Law about the processing of personal data and privacy; |
| “Key Subcontractor” | any Subcontractor:   1. which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or 2. with a Subcontract with a contract value which at the time of appointment exceeds (or would exceed if appointed) ten per cent (10%) of the aggregate Charges forecast to be payable under this Call-Off Contract; |
| “Law” | any applicable Act of Parliament, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of section 2 of the European Communities Act 1972, regulatory policy, guidance or industry code, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply; |
| “Personal Data” | has the meaning given in the UK GDPR; |
| “Purchase Order  Number” | the Authority’s unique number relating to the supply of the Services; |
| “Services” | the services to be supplied by the Supplier to the Authority under the Agreement, including the provision of any Goods; |
| “Subcontract”  “Subcontractor” | any contract or agreement (or proposed contract or agreement) between the Supplier (or a Subcontractor) and any third party whereby that third party agrees to provide to the Supplier (or the Subcontractor) all or any part of the Services, or facilities or services which are material for the provision of the Services, or any part thereof or necessary for the management, direction or control of the Services or any part thereof; |

any third party with whom:

1. the Supplier enters into a Subcontract; or
2. a third party under (a) above enters into a Subcontract, or the servants or agents of that third party;

“Supplier Personnel” all directors, officers, employees, agents, consultants and contractors of

the Supplier and/or of any Subcontractor of the Supplier engaged in the performance of the Supplier’s obligations under the Agreement;

|  |  |  |
| --- | --- | --- |
| “Supporting  Documentation” | | sufficient information in writing to enable the Authority to reasonably verify the accuracy of any invoice; |
| “Tax” |  | 1. all forms of tax whether direct or indirect; 2. national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction; 3. all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions. levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and 4. any penalty, fine, surcharge, interest, charges or costs relating to any of the above,   in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction; |
| “Tax NonCompliance” |  | where an entity or person under consideration meets all 3 conditions contained in the relevant excerpt from HMRC’s “Test for Tax NonCompliance”, as set out in Annex 1, where:   1. the “Economic Operator” means the Supplier or any agent, supplier or Subcontractor of the Supplier requested to be replaced pursuant to Clause 4.3; and 2. any “Essential Subcontractor” means any Key Subcontractor; |
| “UK GDPR” |  | the UK General Data Protection Regulation, the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679); |
| “VAT” |  | value added tax as provided for in the Value Added Tax Act 1994. |

# 2. Payment and Recovery of Sums Due

2.1 The Supplier shall invoice the Authority as specified in the order form/the Agreement. Without prejudice to the generality of the invoicing procedure specified in the Agreement, the Supplier shall procure a Purchase Order Number from the Authority prior to the commencement of any Services and the Supplier acknowledges and agrees that should it commence Services without a Purchase Order Number:

2.1.1 the Supplier does so at its own risk; and

2.1.2 the Authority shall not be obliged to pay any invoice without a valid Purchase Order Number having been provided to the Supplier.

2.2 Each invoice and any Supporting Documentation required to be submitted in accordance with the invoicing procedure specified in the Agreement shall be submitted by the Supplier, as directed by the Authority from time to time via the Authority’s electronic transaction system. 2.3 If any sum of money is recoverable from or payable by the Supplier under the Agreement (including any sum which the Supplier is liable to pay to the Authority in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Supplier under the Agreement or under any other agreement or contract with the Authority. The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Authority in order to justify withholding payment of any such amount in whole or in part.

# 3. Warranties

3.1 The Supplier represents and warrants that:

3.1.1 in the three years prior to the Effective Date, it has been in full compliance with all applicable securities and Laws related to Tax in the United Kingdom and in the jurisdiction in which it is established;

3.1.2 it has notified the Authority in writing of any Tax Non-Compliance it is involved in; and

3.1.3 no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Supplier or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier’s assets or revenue and the Supplier has notified the Authority of any profit warnings issued in respect of the Supplier in the three years prior to the Effective Date.

3.2 If at any time the Supplier becomes aware that a representation or warranty given by it under Clause 3.1.1, 3.1.2 and/or 3.1.3 has been breached, is untrue, or is misleading, it shall immediately notify the Authority of the relevant occurrence in sufficient detail to enable the Authority to make an accurate assessment of the situation.

3.3 In the event that the warranty given by the Supplier pursuant to Clause 3.1.2 is materially untrue, the Authority shall be entitled to terminate the Agreement pursuant to the Call-Off clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

# 4. Promoting Tax Compliance

4.1 All amounts stated are stated exclusive of VAT, which shall be added at the prevailing rate as applicable and paid by the Authority following delivery of a valid VAT invoice.

4.2 To the extent applicable to the Supplier, the Supplier shall at all times comply with all Laws relating to Tax and with the equivalent legal provisions of the country in which the Supplier is established.

4.3 The Supplier shall provide to the Authority the name and, as applicable, the Value Added Tax registration number, PAYE collection number and either the Corporation Tax or self-assessment reference of any agent, supplier or Subcontractor of the Supplier prior to the provision of any material Services under the Agreement by that agent, supplier or Subcontractor. Upon a request by the Authority, the Supplier shall not contract, or will cease to contract, with any agent, supplier or Subcontractor supplying Services under the Agreement.

4.4 If, at any point during the Term, there is Tax Non-Compliance, the Supplier shall:

4.4.1 notify the Authority in writing of such fact within five (5) Working Days of its occurrence; and

4.4.2 promptly provide to the Authority:

1. details of the steps which the Supplier is taking to resolve the Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and
2. such other information in relation to the Tax Non-Compliance as the Authority may reasonably require.
   1. The Supplier shall indemnify the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Authority at any time in respect of the Supplier's failure to account for or to pay any Tax relating to payments made to the Supplier under this Agreement. Any amounts due under this Clause 4.5 shall be paid in cleared funds by the Supplier to the Authority not less than five (5) Working Days before the date upon which the Tax or other liability is payable by the Authority.
   2. Upon the Authority’s request, the Supplier shall provide (promptly or within such other period notified by the Authority) information which demonstrates how the Supplier complies with its Tax obligations.
   3. If the Supplier:
      1. fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with Clauses 4.2, 4.4.1 and/or 4.6 this may be a material breach of the Agreement;
      2. fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with a reasonable request by the Authority that it must not contract, or must cease to contract, with any agent, supplier or

Subcontractor of the Supplier as required by Clause 4.3 on the grounds that the agent, supplier or Subcontractor of the Supplier is involved in Tax Non-Compliance this shall be a material breach of the Agreement; and/or

* + 1. fails to provide details of steps being taken and mitigating factors pursuant to Clause 4.4.2 which in the reasonable opinion of the Authority are acceptable this shall be a material breach of the Agreement;

and any such material breach shall allow the Authority to terminate the Agreement pursuant to the Call-Off Clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

4.8 The Authority may internally share any information which it receives under Clauses 4.3 to 4.4 (inclusive) and 4.6, for the purpose of the collection and management of revenue for which the Authority is responsible.

# 5. Use of Off-shore Tax Structures

5.1 Subject to the principles of non-discrimination against undertakings based either in member countries of the European Union or in signatory countries of the World Trade Organisation Agreement on Government Procurement, the Supplier shall not, and shall ensure that its Connected Companies, Key Subcontractors (and their respective Connected Companies) shall not, have or put in place (unless otherwise agreed with the Authority) any arrangements involving the use of off-shore companies or other off-shore entities the main purpose, or one of the main purposes, of which is to achieve a reduction in United Kingdom Tax of any description which would otherwise be payable by it or them on or in connection with the payments made by or on behalf of the Authority under or pursuant to this Agreement or (in the case of any Key Subcontractor and its Connected Companies) United Kingdom Tax which would be payable by it or them on or in connection with payments made by or on behalf of the Supplier under or

pursuant to the applicable Key Subcontract (“Prohibited Transactions”). Prohibited Transactions shall not include transactions made between the Supplier and its Connected Companies or a Key Subcontractor and its Connected Companies on terms which are at armslength and are entered into in the ordinary course of the transacting parties’ business.

5.2 The Supplier shall notify the Authority in writing (with reasonable supporting detail) of any proposal for the Supplier or any of its Connected Companies, or for a Key Subcontractor (or any of its Connected Companies), to enter into any Prohibited Transaction. The Supplier shall notify the Authority within a reasonable time to allow the Authority to consider the proposed Prohibited Transaction before it is due to be put in place.

5.3 In the event of a Prohibited Transaction being entered into in breach of Clause 5.1 above, or in the event that circumstances arise which may result in such a breach, the Supplier and/or the Key Subcontractor (as applicable) shall discuss the situation with the Authority and, in order to ensure future compliance with the requirements of Clauses 5.1 and 5.2, the Parties (and the Supplier shall procure that the Key Subcontractor, where applicable) shall agree (at no cost to the Authority) timely and appropriate changes to any such arrangements by the undertakings concerned, resolving the matter (if required) through the escalation process in the Agreement.

5.4 Failure by the Supplier (or a Key Subcontractor) to comply with the obligations set out in Clauses 5.2 and 5.3 shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).

# 6 Data Protection and off-shoring

6.1 The parties agree that the Supplier shall, whether it is the Controller or Processor, in relation to any Personal Data processed in connection with its obligations under the Agreement:

6.1.1 not process or permit to be processed Personal Data outside of the United Kingdom unless the prior explicit written consent of the Authority has been obtained and the following conditions are fulfilled:

1. the Supplier or any applicable Processor has provided appropriate safeguards in relation to any transfer of the Personal Data (whether in accordance with UK GDPR Article 46 or, where relevant, section 75 of the Data Protection Act 2018) as determined by either the Authority or the Supplier when it is the Controller;
2. the Data Subject has enforceable rights and effective legal remedies;
3. the Supplier or any applicable Processor complies with its obligations under the Data

Protection Legislation by providing an adequate level of protection to any Personal Data that is processed (or, if it is not so bound, uses its best endeavours to assist either the Authority or the Supplier when it is the Controller in meeting its obligations); and

1. the Supplier or any applicable Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

6.2 Failure by the Supplier to comply with the obligations set out in Clause 6.1 shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

# 7 Commissioners for Revenue and Customs Act 2005 and related Legislation

7.1 The Supplier shall comply with, and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in Section 18 of the Commissioners for Revenue and Customs Act 2005 (‘CRCA’) to maintain the confidentiality of Authority Data. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the aforesaid obligations may lead to a prosecution under Section 19 of CRCA.

7.2 The Supplier shall comply with, and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in Section 123 of the Social Security Administration Act 1992, which may apply to the fulfilment of some or all of the Services. The Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the Supplier’s obligations under Section 123 of the Social Security Administration Act 1992 may lead to a prosecution under that Act.

7.3 The Supplier shall regularly (not less than once every six (6) months) remind all Supplier Personnel who will have access to, or are provided with, Authority Data in writing of the obligations upon Supplier Personnel set out in Clause 7.1 above. The Supplier shall monitor the compliance by Supplier Personnel with such obligations.

7.4 The Supplier shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data sign (or have previously signed) a Confidentiality Declaration, in the form provided at Annex 2. The Supplier shall provide a copy of each such signed declaration to the Authority upon demand.

7.5 In the event that the Supplier or the Supplier Personnel fail to comply with this Clause 7, the Authority reserves the right to terminate the Agreement with immediate effect pursuant to the clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).

Annex 1

Excerpt from HMRC’s “Test for Tax Non-Compliance”

Condition one (An in-scope entity or person)

1. There is a person or entity which is either: (“X”)

1. The Economic Operator or Essential Subcontractor (EOS)
2. Part of the same Group of companies of EOS. An entity will be treated as within the same Group of EOS where that entities’ financial statements would be required to be consolidated with those of EOS if prepared in accordance with IFRS 10 Consolidated Financial Accounts1;
3. Any director, shareholder or other person (P) which exercises control over EOS. ‘Control’ means P can secure, through holding of shares or powers under articles of association or other document that EOS’s affairs are conducted in accordance with P’s wishes.

Condition two (Arrangements involving evasion, abuse or tax avoidance)

2. X has been engaged in one or more of the following:

1. Fraudulent evasion2;
2. Conduct caught by the General Anti-Abuse Rule[[1]](#footnote-2);
3. Conduct caught by the Halifax Abuse principle[[2]](#footnote-3);
4. Entered into arrangements caught by a DOTAS or VADR scheme[[3]](#footnote-4);
5. Conduct caught by a recognised ‘anti-avoidance rule’[[4]](#footnote-5) being a statutory provision which targets arrangements where either a main purpose, or an expected benefit, is to obtain a tax advantage or where the arrangement is not affected for commercial purposes. ‘Targeted AntiAvoidance Rules’ (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;
6. Entered into an avoidance scheme identified by HMRC’s published Spotlights list[[5]](#footnote-6);

1. https://www.iasplus.com/en/standards/ifrs/ifrs10
2. ‘Fraudulent evasion’ means any ‘UK tax evasion offence’ or ‘UK tax evasion facilitation offence’ as defined by section 52 of the Criminal Finances Act 2017 or a failure to prevent facilitation of tax evasion under section 45 of the same Act.

g. Engaged in conduct which falls under rules in other jurisdictions which are equivalent or similar to (a) to (f) above.

Condition three (Arrangements are admitted, or subject to litigation/prosecution or identified in a published list (Spotlights))

3. X’s activity in Condition 2 is, where applicable, subject to dispute and/or litigation as follows:

* 1. In respect of (a), either X:
     1. Has accepted the terms of an offer made under a Contractual Disclosure Facility (CDF) pursuant to the Code of Practice 9 (COP9) procedure[[6]](#footnote-7); or,
     2. Has been charged with an offence of fraudulent evasion.
  2. In respect of (b) to (e), once X has commenced the statutory appeal process by filing a Notice of Appeal and the appeal process is ongoing including where the appeal is stayed or listed behind a lead case (either formally or informally). NB Judicial reviews are not part of the statutory appeal process and no supplier would be excluded merely because they are applying for judicial review of an HMRC or HMT decision relating to tax or national insurance.
  3. In respect of (b) to (e), during an HMRC enquiry, if it has been agreed between HMRC and X that there is a pause with the enquiry in order to await the outcome of related litigation.
  4. In respect of (f) this condition is satisfied without any further steps being taken.
  5. In respect of (g) the foreign equivalent to each of the corresponding steps set out above in (i) to (iii).

For the avoidance of doubt, any reference in this Annex 1 to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time including any implementing or successor legislation.

Annex 2 Form

CONFIDENTIALITY DECLARATION CONTRACT REFERENCE: SR1061995109. 22/11/22 ‘the Agreement’)

DECLARATION:

I solemnly declare that:

1. I am aware that the duty of confidentiality imposed by section 18 of the Commissioners for Revenue and Customs Act 2005 applies to Authority Data (as defined in the Agreement) that has been or will be provided to me in accordance with the Agreement.
2. I understand and acknowledge that under Section 19 of the Commissioners for Revenue and Customs Act 2005 it may be a criminal offence to disclose any Authority Data provided to me.

|  |
| --- |
| SIGNED: Redacted |
| FULL NAME: xxxxx xxxxxxxxx |
| POSITION: SENIOR ACCOUNT MANAGER |
| COMPANY: AMR Cyber Security Ltd |
| DATE OF SIGNATURE: |

1. “General Anti-Abuse Rule” means (a) the legislation in Part 5 of the Finance Act 2013; and (b) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions [↑](#footnote-ref-2)
2. “Halifax Abuse Principle” means the principle explained in the CJEU Case C-255/02 Halifax and others [↑](#footnote-ref-3)
3. A Disclosure of Tax Avoidance Scheme (DOTAS) or VAT Disclosure Regime (VADR) scheme caught by rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Section 19 and Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Section 19 and Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992. [↑](#footnote-ref-4)
4. The full definition of ‘Anti-avoidance rule’ can be found at Paragraph 25(1) of Schedule 18 to the Finance Act 2016 and Condition 2 (a) above shall be construed accordingly. [↑](#footnote-ref-5)
5. Targeted list of tax avoidance schemes that HMRC believes are being used to avoid paying tax due and which are listed on the Spotlight website: https://www.gov.uk/government/collections/tax-avoidance-schemescurrently-in-the-spotlight [↑](#footnote-ref-6)
6. The Code of Practice 9 (COP9) is an investigation of fraud procedure, where X agrees to make a complete and accurate disclosure of all their deliberate and non-deliberate conduct that has led to irregularities in their tax affairs following which HMRC will not pursue a criminal investigation into the conduct disclosed. [↑](#footnote-ref-7)