**CYBER SECURITY SERVICES 2 (RM3764ii)**

**VARIATION FORM**

Variation Form No:

……………………………………………………………………………………

BETWEEN:

|  |
| --- |
| **Crown Commercial Service** (**the Authority CCS**)  and  **[**insert name of Supplier**]** (**the Supplier**) |

1. The Cyber Security Services 2 (RM3764ii) Framework Agreement is varied as follows and shall take effect on the date signed by both Parties:

Refer to Annex 1 hereto

1. Words and expressions in this Variation shall have the meanings given to them in this Framework Agreement.
2. This Framework Agreement, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.
3. 12/08/2013

Signed by an authorised signatory for and on behalf of CCS

|  |  |
| --- | --- |
| Signature |  |
| Date |  |
| Name (in Capitals) |  |
| Address | Crown Commercial Service, Rosebery Court, St Andrews |
|  | Business Park, Norwich, NR7 0HS |

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

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

**ANNEX 1**

**Framework Agreement**

**Table of Contents**

1) “Schedules” - add “5 - Schedule of Processing, Personal Data and Data Subjects”

**Terms and Conditions**

1) Delete Clause 40.4 “Protection of Personal Data” and insert the following as new Clause 40.4 “Data Protection”

* + 1. “The Parties acknowledge that for the purposes of the Data Protection Legislation, CCS is the Controller and the Supplier is the Processor. The only processing that the Supplier is authorised to do is listed in Schedule 5 by CCS and may not be determined by the Supplier.
    2. The Supplier shall notify CCS immediately if it considers that any of CCS’ instructions infringe the Data Protection Legislation.
    3. The Supplier shall provide all reasonable assistance to CCS in the preparation of any Data Protection Impact Assessment prior to commencing any processing.  Such assistance may, at the discretion of CCS, include:
       1. a systematic description of the envisaged processing operations and the purpose of the processing;
       2. an assessment of the necessity and proportionality of the processing operations~~;~~
       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 Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Framework Agreement:
       1. process that Personal Data only in accordance with Schedule 5 unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify CCS before processing the Personal Data unless prohibited by Law;
       2. ensure that it has in place Protective Measures, which have been reviewed and approved by CCS as appropriate to protect against a Data Loss Event having taken account of the:

1. nature of the data to be protected;
2. harm that might result from a Data Loss Event;
3. state of technological development; and
4. cost of implementing any measures;
   * + 1. ensure that :
          1. the Supplier Personnel do not process Personal Data except in accordance with this Framework Agreement (and in particular Schedule 5);
          2. it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:
5. are aware of and comply with the Supplier’s duties under this clause;
6. are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;
7. 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 CCS or as otherwise permitted by this Framework Agreement; and
8. have undergone adequate training in the use, care, protection and handling of Personal Data; and
   * + 1. not transfer Personal Data outside of the European Economic Area unless the prior written consent of CCS has been obtained and the following conditions are fulfilled:
9. CCS or the Supplier has provided appropriate safeguards in relation to the transfer;
10. the Data Subject has enforceable rights and effective legal remedies;
11. the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
12. the Supplier complies with any reasonable instructions notified to it in advance by CCS with respect to the processing of the Personal Data;
    * + 1. at the written direction of CCS, delete or return Personal Data (and any copies of it) to CCS on termination of the Framework Agreement unless the Supplier is required by Law to retain the Personal Data.
      1. Subject to clause 40.4.6, the Supplier shall notify CCS immediately if 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 eer 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 this Framework Agreement;
         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 Data Loss Event.
      2. The Supplier’s obligation to notify under clause 40.4.5 shall include the provision of further information to CCS in phases, as details become available.
      3. Taking into account the nature of the processing, the Supplier shall provide CCS with full assistance  in relation to either party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 40.4.5 (and insofar as possible within the timescales reasonably required by CCS) including by promptly providing:
         1. CCS with full details and copies of the complaint, communication or request;
         2. such assistance as is reasonably requested by CCS to enable CCS to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
         3. CCS, at its request, with any Personal Data it holds in relation to a Data Subject;
         4. assistance as requested by CCS following any Data Loss Event;
         5. assistance as requested by CCS with respect to any request from the Information Commissioner’s Office, or any consultation by CCS with the Information Commissioner's Office.
      4. The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:
         1. CCS determines that the processing is not occasional;
         2. CCS determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
         3. CCS determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
      5. The Supplier shall allow for audits of its Data Processing activity by CCS or CCS’ designated auditor.
      6. The Supplier shall designate a data protection officer if required by the Data Protection Legislation.
      7. Before allowing any Sub-processor to process any Personal Data related to this Framework Agreement, the Supplier must:
         1. notify CCS in writing of the intended Sub-processor and processing;
         2. obtain the written consent of CCS;
         3. enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 40.4 such that they apply to the Sub-processor; and
         4. provide CCS with such information regarding the Sub-processor as CCS may reasonably require.
      8. The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.
      9. CCS may, at any time on not less than 30 Working Days’ notice, revise this clause 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 this Framework Agreement).
      10. The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner’s Office publishes guidance. CCS may on not less than 30 Working Days’ notice to the Supplier amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner’s Officer. “

2) Correct the following cross-reference in Clause 23.11.1 Consequences of Suspension, Termination and Expiry:

Change “41.4 (Protection of Personal Data)” to “40.4 (Data Protection)”

**Schedule 3 Part C Call-Off Contract Standard Terms**

1) Delete the following definitions from Clause 47 Glossary

“Data Controller”

“Data Processor”

“Data Protection Legislation or DPA”

“Data Subject”

“Personal Data”

2) Insert the following definitions:

**Controller** takes the meaning given in the Data Protection Legislation.

**Data Loss Event**: any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Framework Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Framework Agreement, including any Personal Data Breach**.**

**Data Protection Legislation**: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iiii) all applicable Law about the processing of personal data and privacy;

**Data Protection Impact Assessment:** an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

**Data Protection Officer** takes the meaning given in the Data Protection Legislation.

**Data Subject** takes the meaning given in the Data Protection Legislation.

**Data Subject Access Request**: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

**DPA 2018:** means theData Protection Act 2018

**GDPR**:the General Data Protection Regulation (*Regulation (EU) 2016/679*)

**LED:**Law Enforcement Directive (*Directive (EU) 2016/680*)

**Personal Data** takes the meaning given in the Data Protection Legislation.

**Personal Data Breach** takes the meaning given in the Data Protection Legislation.

**Processor** takes the meaning given in the Data Protection Legislation.

**Protective Measures:** appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it.

**Sub-processor**: any third party appointed to process Personal Data on behalf of the Supplier under this Framework Agreement

3) In the definition of “Customer Data” change “Data Controller” to “Controller”

**Framework Agreement Schedule 4 Definitions & Interpretation**

1) Delete the following definitions:

“Data Controller”

“Data Processor”

“Data Protection Legislation” or “DPA”

“Data Subject”

“Data Subject Access Request”

“Personal Data”

“Processing”

“Service Personal Data”

2) Insert the following definitions:

**Data Loss Event**: any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Call-Off Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Call-Off Contract, including any Personal Data Breach**.**

**Data Protection Legislation**: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iiii) all applicable Law about the processing of personal data and privacy;

**Data Protection Impact Assessment:** an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

**Data Protection Officer** takes the meaning given in the Data Protection Legislation

**Data Subject** takes the meaning given in the Data Protection Legislation

**Data Subject Access Request**: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

**DPA 2018:** means theData Protection Act 2018

**GDPR**:the General Data Protection Regulation (*Regulation (EU) 2016/679*)

**LED:**Law Enforcement Directive (*Directive (EU) 2016/680*)

**Personal Data** takes the meaning given in the Data Protection Legislation.

**Personal Data Breach** takes the meaning given in the Data Protection Legislation

**Processor** takes the meaning given in the Data Protection Legislation

**Protective Measures:** appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it.

**Sub-processor**: any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract

**Framework Schedule 5 Schedule of Processing, Personal Data and Data Subjects**

1. Add the following new Schedule 5

|  |  |
| --- | --- |
| **Description** | **Details** |
| Subject matter of the processing | Management of the Cyber Security 2 Framework Agreement between the Authority and the Supplier |
| Duration of the processing | Up to 7 years after the expiry or termination of the Framework Agreement |
| Nature and purposes of the processing | To facilitate the fulfilment of the Supplier’s obligations arising under this Framework Agreement including   1. Ensuring effective communication between the Supplier and the Authority 2. Maintaining full and accurate records of every Call-Off Contract arising under the Framework Agreement in accordance with Clause 44 ( Records & Audit Access) |
| Type of Personal Data | Includes:   1. Contact details of, and communications with, Authority staff concerned with management of the Framework Agreement 2. Contact details of, and communications with, Customer staff concerned with award and management of Call-Off Contracts awarded under the Framework Agreement, 3. Contact details, and communications with, Sub-contractor staff concerned with fulfilment of the Supplier’s obligations arising from this Framework Agreement |
| Categories of Data Subject | Includes:   1. Authority staff concerned with management of the Framework Agreement 2. Customer staff concerned with award and management of Call-Off Contracts awarded under the Framework Agreement 3. Sub-contractor staff concerned with fulfilment of the Supplier’s obligations arising from this Framework Agreement |
| Plan for return or destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data | All relevant data to be deleted 7 years after the expiry or termination of this Framework Agreement unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder |