Crown Commercial Service

CONSTRUCTION PROFESSIONAL SERVICES FRAMEWORK SCHEDULE 5

TEMPLATE CALL OFF AGREEMENT (INCORPORATING THE NEC4 PROFESSIONAL SERVICES CONTRACT JUNE 2017 (INCLUDING AMENDMENTS ISSUED JANUARY 2019 AND OCTOBER 2020), CONTRACT DATA AND Z CLAUSES

TABLE OF CONTENTS

Date 12th December 2022

FORM OF AGREEMENT

Incorporating the NEC4 Professional Services Contract June 2017 incorporating amendments January 2019 and October 2020

Between

The Department for Work and Pensions ("DWP")

And

TETRA TECH LIMITED

For the provision of

Professional Services to deliver a Flood Risk Assessment in FY2022/23

THIS AGREEMENT is made the 12th day December 2022

PARTIES:

1. **THE DEPARTMENT FOR WORK AND PENSIONS** acting as part of the Crown (the ***"Client***"); and

2. **TETRA TECH LIMITED,** which is a company incorporated in and in accordance with the laws of England and Wales (Company No. 1959704 whose registered office address is at Quay West at MediaCityUK, Trafford Wharf Rd, Trafford Park, Manchester M17 1HH (the ***"Consultant"***).

BACKGROUND

(A) The Minister for the Cabinet Office (the "**Cabinet Office**") as represented by Crown Commercial Service, a trading fund of the Cabinet Office, without separate legal personality (the "**Authority**"), established a framework for construction professional services for the benefit of public sector bodies.

IT IS AGREED AS FOLLOWS:

1. The *Client* will pay the *Consultant* the amount due and carry out his duties in accordance with the *conditions of contract* identified in the Contract Data and the Contract Schedules.

2. The *Consultant* will Provide the Service in accordance with the *conditions of contract* identified in the Contract Data and the Contract Schedules.

3. This contract incorporates the conditions of contract in the form of the NEC4 Professional Services Contract June 2017 Edition incorporating amendments January 2019 and October 2020 and incorporating the following Options:

    - Main Option A;
    - Dispute Resolution Option W2;
    - Secondary Options X2, X10, X11, X18, and X20

    Option Y(UK)2 Together with the following Contract Schedules:

    1. Contract Schedule 1 – Statement of Requirements and Scope
    2. Contract Schedule 2 - Consultant Proposal
    3. Contract Schedule 3 – Activity Schedule
    4. Contract Schedule 4 - Government Commercial Function Supplier Code of Conduct
    5. Contract Schedule 5 - DWP Security Policy
    6. Contract Schedule 6 - Key Performance Indicators
    7. Contract Schedule 7 - Financial Distress
    8. Contract Schedule 8 – GDPR

    which together with the *additional conditions of contract* specified in Option Z, and the amendments specified in Option Z, form this contract together with the documents referred to in it. References in the NEC4 Professional Services Contract June 2017

Edition incorporating amendments January 2019 and October 2020 to "the contract" are references to this contract.

4. This contract and the Framework Agreement is the entire agreement between the parties in relation to the *service* and supersedes and extinguishes all prior arrangements, understandings, agreements, statements, representations, or warranties (whether written or oral) relating thereto.

5. Neither party has been given, nor entered into this contract in reliance on any arrangements, understandings, agreements, statements, representations or warranties other than those expressly set out in this agreement.

6. Nothing in clauses 4 or 5 shall exclude liability in respect of misrepresentations made fraudulently.

Executed under hand

Signed by REDACTED for and on behalf of **TETRA TECH LIMITED**

REDACTED

The Client

Signed by REDACTED for an on behalf of The Secretary of State for Work and Pensions of Caxton House, Tothill Street, London, SW1H 9NA

REDACTED

REDACTED

Authorised Signatory

Professional Services Contract
Contract Data

Part one – Data provided by the *Client*

1 General

The *conditions of contract* are the core clauses and the clauses for the following main option, the option for resolving and avoiding disputes and the and secondary Options of the NEC4 Professional Services Contract June 2017 incorporating amendments January 2019 and October 2020.

Main Option A

Option for resolving and avoiding disputes W2

Secondary Options X1, X2, X3, X4, X5, X6, X7, X8, X9, X10, X11, X12, X13, X18, X20, Y(UK)2 and Z.

- The *service* is as set out in The Statement of Requirements and

Scope appended to this agreement.

- The *Client* is Department for Work and Pensions of Caxton House, Tothill Street, London, SW1H 9NA.

Address for communications

Caxton House, Tothill Street, London, SW1H 9NA

Address for electronic communications

REDACTED

REDACTED

The ***Service Manager*** is REDACTED *and* REDACTED

Address for communications

Department for Work and Pensions, Ground Floor, Caxton House, Tothill Street, London, SW1H 9NA

Address for electronic communications

REDACTED

REDACTED

The Scope is as in The Statement of Requirements and Scope (Contract Schedule 1) appended to this agreement.

The *language of the contract* is English.

The law of the contract is the law of England and Wales and the Courts of the country selected above, shall have exclusive jurisdiction with regard to any dispute in connection with this Agreement and the Parties irrevocably agree to submit to the jurisdiction of those courts.

If Option Y(UK)2 is said to apply then notwithstanding that this contract relates to the carrying out of construction operations other than in England or Wales or Scotland, the Act is deemed to apply to this contract.

The *period for reply* is two weeks.

The *period for retention* is 6 years following Completion or earlier termination.

The following matters will be included in the Early Warning Register

N/A

Early warning meetings are held at intervals no longer than two weeks

2 The *Consultant's* main responsibilities

If the Client has identified work which is set to meet a stated *condition* by a *key date*

The *key dates* and *conditions* to be met are

condition to be met	*key date*
Completion of progress reports and attendance at progress meeting(s)	within timescales communicated in writing (which may include email) by the Client to the Consultant as and when required
Project Data Gathering	All third party data will be requested from the Environment Agency by 23/12/22
Develop flood plans, including maps, preparation for floods, and any recommended measures for protecting buildings	17/03/23
Flood plan Report and Handover	31/03/23

If Option A is used

The *Consultant* prepares forecasts of the total *expenses* at intervals no longer than 2 weeks

3 Time

The starting date is 12th December 2022

The *Client* provides access to the following persons, places, and things

- access to *access date*

access to DWP premises as necessary.

The *Consultant* submits revised programmes at intervals no longer than one week.

If the *Client* has decided the *completion date* for the whole of the *service*

The *completion date* for the whole of the *service* is 31st March 2023

4 Quality Management

The period after the Contract Date within which the *Consultant* is to submit a quality policy statement and quality plan is 2 weeks

The period between Completion of the whole of the *service* and the *defects date* is 52 weeks

5 Payment

The *currency of the contract* is the pound sterling (£).

The *assessment interval* is monthly

If the *Client* states any *expenses*

The *expenses* stated by the *Client* are

Item	Amount
n/a	

The *interest rate* is, 3% per annum above the Bank of England base rate in force from time to time.

6 Compensation events

If there are additional compensation events

These are additional compensation events

N/A

8 Liability and insurance

If there are additional *Client* liabilities

These are additional *Client* liabilities

1 N/A

The amounts of insurance and the periods for which the *Consultant* maintains insurance are

event	cover	Period

The Consultant's failure to use the skill and care normally used by professionals providing services similar to the service 1.*Professional Indemnity Insurance* - To indemnify the insured for all sums which the insured shall become legally liable to pay (including claimants' costs and expenses) as a result of claims first made against the insured during the period of insurance by reason of any negligent act, error and/or omission arising from or in connection with the performance of its obligations under the Framework Alliance Contract.	Not less than £1,000,000 in respect of each claim, without limit to the number of claims except for claims arising out of pollution or contamination, where the minimum amount of cover applies in the aggregate in any one period of insurance and except for claims arising out of asbestos where a lower level may apply in the aggregate. Not less than £2,000,000 in respect of any one occurrence, the number of occurrences being unlimited, but £2,000,000 any one occurrence and in the aggregate per annum in respect of products and pollution liability.	From the date of the Framework Alliance Contract and renewable on an annual basis unless agreed otherwise by the Client in writing (a) throughout the Framework Period or until earlier termination of the Framework Alliance Contract and (b) for a period of 6 years thereafter.
2. *Third Party Public Liability Insurance* - To indemnify the insured in respect of all sums which the insured shall become legally liable to pay as damages, including claimant's costs and expenses, in respect of accidental: ● death or bodily injury to or sickness, illness or disease		

contracted by any person;

● loss of or damage to property;

happening during the period of insurance and arising out of or in connection with any matter governed by the Framework Alliance Contract.

The Consultant's total liability to the Client for all matters arising under or in connection with the contract, other than the excluded matters, is limited to £1,000,000 in the aggregate.

Resolving and avoiding disputes

The *tribunal* is arbitration

If the *tribunal* is arbitration

The arbitration procedure is the London Court of International Arbitration Rules;

The place where arbitration is to be held is London

The person or Organisation who will choose the arbitrator if the parties cannot agree a choice or if the arbitration procedure does not state who selects and arbitrator is: Royal Institution of Chartered Surveyors.

The *Representatives* of the *Client* are:

REDACTED

REDACTED

REDACTED

Address for communications:

Department for Work and Pensions I Ground Floor, Caxton House, Tothill Street, London, SW1H 9NA

Address for electronic communications:

REDACTED

REDACTED

REDACTED

The *Senior Representatives* of the *Client* are:

Siobhan Walker and Nicola Oxley

Address for communications:

Department for Work and Pensions I Ground Floor, Caxton House, Tothill Street, London, SW1H 9NA

Address for electronic communications:

REDACTED and REDACTED

The representative of the *Consultant* is*:* REDACTED

Address for communications: Quay West at MediaCityUK, Trafford Wharf Rd, Trafford Park, Manchester M17 1HH

Address for electronic communications: REDACTED

The Senior Representative of the *Consultant* is: REDACTED

Address for communications: Quay West at MediaCityUK, Trafford Wharf Rd, Trafford Park, Manchester M17 1HH

Address for electronic communications: REDACTED

The *Adjudicator* is the person agreed by the Parties from the list of *Adjudicator*s published by the Royal Institution of Chartered Surveyors or nominated by the *Adjudicator nominating body* in the absence of agreement.

Address for communications [To be provided on agreement of adjudicator]

Address for electronic communications [To be provided on agreement of adjudicator]

The Adjudicator nominating body is the Royal Institute of Chartered Surveyors.

Option X1 **Option X1 is not used**

Option X2 Changes in the law **If Option X2 is used**

The law of the project is the law of England and Wales

Option X3 **Option X3 is not used**

Option X5 **Option X5 is not used**

Option X6 **Option X6 is not used**

Option X7 **Option X7 is not used**

Option X8 **Option X8 is not used**

Option X10 Information modelling **If Option X10 is used**

If no *information execution plan* is identified in part two of the Contract Data

The period after the Contract Date within which the *Consultant* is to submit a first Iinformation Execution Plan for acceptance is 2 weeks

Option X12 **Option X12 is not used**

Option X13 **Option X13 is not used**

Option X18 Limitation of liability **If Option X18 is used**

- The Consultant's liability to the Employer for indirect or consequential loss is limited to £1,000,000.
- The Consultant's total liability to the Employer for all matters arising under or in connection with the contract, other than excluded matters, is limited to £1,000,000.
- The end of liability date is 6 years after Completion of the whole of the services.

Option X20 Key performance indicators **If Option X20 is used**

The incentive schedule for Key Performance Indicators is in Schedule 6

A report of performance against each Key Performance Indicator is provided at intervals of 1 month.

Where X20 is used, the amount due under clause 50 is adjusted to account for the application of the *incentive schedule.*

Option Y(UK)1 **Y(UK)1 is not used**

Option Y(UK)3 **Y(UK)3 is not used**

Option Z The *additional conditions of contract* are: Z9, Z19, Z22, Z35, Z36, Z37, Z41 and Z48

Contract Data relating to Z clauses The additional conditions of contract are as selected below and as detailed in the appended Standard Boilerplate Amendments.

Option Z2 **Definitions**

does not apply

Option Z4 **Admittance to Client's Premises**

does not apply

Option Z5 **Prevention of fraud and bribery**

does not apply

Option Z6 **Equality and diversity**

does not apply

Option Z7 **Legislation and Official Secrets**

does not apply

Option Z8 **Conflict of interest**

does not apply

Option Z9 **Publicity and Branding**

applies

Option Z10 **Freedom of information**

does not apply

Option Z13 **Confidentiality and Information Sharing**

does not apply]

Option Z14 **Security Requirements**

does not apply

Option Z16 **Tax Compliance**

does not apply

Option Z22 **Fair payment**

applies

Option Z42 **The Housing Grants, Construction and Regeneration Act 1996**

does not apply

Option Z44 **Intellectual Property Rights**

does not apply

Option Z45 **HMRC Requirements**

does not apply

Option Z46 **MoD DEFCON Requirements**

does not apply

Option Z47 **Small and Medium Sized Enterprises (SMEs)**

does not apply

Option Z48 **Apprenticeships**

applies

Option Z49	**Change of Control** does not apply
Option Z50	**Financial Standing** does not apply
Option Z51	**Financial Distress** does not apply
Option Z52	**Records, audit access and open book data** does not apply
Option Z100	**Data Protection** does not apply
Option Z101	**Cyber Essentials** applies
Other *Additional conditions of contract*	n/a

Part two – Data provided by the *Consultant*

1 Statements given in all contracts

The *Consultant* is Tetra Tech Limited

Address for communications *Tetra Tech, Quay West at MediaCityUK, Trafford Wharf Rd, Trafford Park, Manchester M17 1HH*

Address for electronic communications REDACTED

The *key persons* are

REDACTED

The following matters will be included in the Early Warning Register

- Any delays related to setting up licensing of Government data for use by Tetra Tech on behalf of DWP.
- Resourcing requirements and any impacts of CV-19 on project programme.
- Access to any additional DWP data required for Tasks 1 to 3.

  Task 1 : Project Inception and Data Gathering

  Task 2 : Flood Plans for 38 sites

  Task 3 : Project Management, Reporting and Handover

  Access to offices and staff for Task Site Visits for 38 sites

2 The *Consultant's* main responsibilities

If the Consultant is to provide the Scope

The Scope provided by the *Consultant* is in n/a

3 Time

If a programme is to be identified in the Contract Data

The programme identified in the Contract Data is as per the proposal in Contract Schedule 2

If the *Consultant* is to decide the *completion date* for the whole of the *service*

The *completion date* for the whole of the *service* is 31st March 2023

5 Payment

If the *Consultant* states any *expenses*

The *expenses* stated by the *Consultant* are

• **item**	• **amount**
• Expenses for site visits to up to four Client sites unless further site visits are requested by the Client in line with the Statement of Requirements and Scope.	The amount due to the Consultant for expenses will be limited to the expenses properly spent by the Consultant in providing the Services in line with the Client's Expenses Policy

The amount due to the Consultant for expenses will be limited to the expenses properly spent by the Consultant in providing the Services in line with the Client's Expenses Policy in Contract Schedule 1

If Option A or C is used

The *activity schedule* is defined in the proposal and includes 3 main tasks:

Task 1 : Project Inception and Data Gathering

Task 2 : Flood Plans for 38 sites

Task 3 : Project Management, Reporting and Handover

The tendered total of the Prices is:

REDACTED

Resolving and avoiding disputes

The *Representatives* of the *Consultant* are

REDACTED

Quay West at MediaCityUK, Trafford Wharf Rd, Trafford Park, Manchester M17 1HH

REDACTED

The *Senior Representatives* of the *Consultant* are

REDACTED

Quay West at MediaCityUK, Trafford Wharf Rd, Trafford Park, Manchester M17 1HH

REDACTED

Option X10 Information modelling	**If Option X10 is used**
If an *information execution plan* is to be identified in the Contract Data	The Information Execution Plan identified in the Contract Data is n/a
Option Y(UK)1 Project bank account	**If Option Y(UK)1 is not used**
Data for the Schedule of Cost Components (used only with Options A and C)	The *overhead percentages* for the cost of support people and office overhead are location *overhead percentage* n/a
Data for the Schedule of Cost Components (used only with Option A)	The *people rates* are as follows based on 8 hour day:

- REDACTED
- REDACTED

Payments

- **Dec-22** 45% of contract value REDACTED
- **Feb-22** 45% of contract value REDACTED
- **Mar-22** 10% on completion of all tasks (retention) REDACTED
- REDACTED

Contract Schedule 1 - The Statement of Requirements (Scope)

DWP Flood Risk Assessments EOI

Contract Schedule 2 - Tetra Tech Ltd response to EOI

Quality question PROJ1.1 – Method Statement(s)

- REDACTED

Quality question PROJ1.2 – Project Team & Approach to service delivery

- REDACTED

Contract Schedule 3 – Activity Schedule

- REDACTED

Contract Schedule 4 - Government Commercial Function Supplier Code of Conduct

You can find the latest version of the Supplier Code of Conduct published on: https://www.gov.uk/government/publications/supplier-code-of-conduct unless specified otherwise

Contract Schedule 5 - DWP Security Policy

1. GENERAL

The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, comply with the Employer's security requirements as set out in the Call Off Contract which include the requirements set out in this Schedule 8 to the Call Off Contract (the "**Security Policy**"). The Security Policy includes, but is not limited to, requirements regarding the confidentiality, integrity and availability of Employer Assets, the Employer's Systems Environment and the Consultant's Systems Environment.
Terms used in this Schedule 8 which are not defined below shall have the meanings given to them in the Contract Data and/or clause Z1 (Interpretation and the law) of this Call Off Contract.

"**Availability Test**"	shall mean the activities performed by the Consultant to confirm the availability of any or all components of any relevant ICT system as specified by the Employer.
"**Breach of Security**"	means the occurrence of: (I) any unauthorised access to or use of Employer Data, the Employer's Systems Environment (or any part thereof) or the Consultant's Systems Environment (or any part thereof); (II) the loss and/or unauthorised disclosure of any Employer Data, the Employer's Systems Environment (or any part thereof) or the Consultant's Systems Environment (or any part thereof); (III) any unauthorised event resulting in loss of availability of any Employer Data, the Employer's Systems Environment (or any part thereof) or the Consultant's Systems Environment (or any part thereof); (IV) any unauthorised changes or modification to any Employer Data, the Employer's Systems Environment (or any part thereof)

	or the Consultant's Systems Environment (or any part thereof).
"**CHECK**"	shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.
"**Cloud**"	shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data.
"**Consultant's Systems Environment**"	means any ICT systems provided by the Consultant (and any Sub-consultant) which are or may be used for the provision of the *services*.
"**Cyber Essentials**"	shall mean the Government-backed, industry-supported scheme managed by the NCSC to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
"**Cyber Security Information Sharing Partnership**" or "**CiSP**"	shall mean the cyber security information sharing partnership established by the NCSC or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
"**Employer Assets**"	mean any *Employer* Devices and *Employer* Data.
"**Employer Data**"	means the data, guidance, specifications, instructions, toolkits, plans, databases, patents, patterns, models, design, 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:- (i) supplied to the *Consultant* by or on behalf of the Employer; or (ii) which the *Consultant* is required to generate, process, store or transmit pursuant to this Call Off Contract.

"**Employer's Systems Environment**"	means all of the Employer's ICT systems which are or may be used for the provision of the *services*.
"**Good Security Practice**"	shall mean: a) the technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for Standardization or the National Institute of Standards and Technology); b) security standards and guidelines relating to Information Security (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) provided to the general public or Information Security practitioners and stakeholders by generally recognised authorities and organisations; and c) the Government's security policies, frameworks, standards and guidelines relating to Information Security.
"**Information Security**"	shall mean: a) the protection and preservation of: i) the confidentiality, integrity and availability of any Employer Assets, the Employer's Systems Environment (or any part thereof) and the Consultant's Systems Environment (or any part thereof); ii) related properties of information including, but not limited to, authenticity,

	accountability, and non-repudiation; and b) compliance with all Law applicable to the processing, transmission, storage and disposal of Employer Assets.
"**Information Security Manager**"	shall mean the person appointed by the Consultant with the appropriate experience, authority and expertise to ensure that the Consultant complies with the Security Policy.
"**Information Security Management System ("ISMS")**"	shall mean the set of policies, processes and systems designed, implemented and maintained by the Consultant to manage Information Security Risk as certified by ISO/IEC 27001.
"**Information Security Questionnaire**"	shall mean the Employer's set of questions used to audit and on an ongoing basis assure the Consultant's compliance with the Security Policy. The Information Security Questionnaire is the Security Management Plan.
"**Information Security Risk**"	shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.
"**ISO/IEC 27001, ISO/IEC 27002 and ISO 22301**	shall mean a) ISO/IEC 27001; b) ISO/IEC 27002/IEC; and c) ISO 22301 in each case as most recently published by the International Organization for Standardization or its successor entity (the "**ISO**") or the relevant successor or replacement information security standard which is formally recommended by the ISO.
"**NCSC**"	shall mean the National Cyber Security Centre or its successor entity (where applicable).
"**Penetration Test**"	shall mean a simulated attack on any Employer Assets, the Employer's Systems Environment (or any part thereof) or the

	Consultant's Systems Environment (or any part thereof).
"**PCI DSS**"	shall mean the Payment Card Industry Data Security Standard as most recently published by the PCI Security Standards Council, LLC or its successor entity (the "**PCI**").
"**Risk Profile**"	shall mean a description of any set of risk. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable.
"**Security Test"**	shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.
"**Security Policies**"	means the Employer's security policy attached as a Contract Schedule as may be updated from time to time
"**Security Policies and Standards**"	mean the Security Policies and the Security Standards. Security Policies are set out in Annex A.
"**Security Standards**"	mean the Employer's Security Standards published by the Employer from time to time and shall include any successor, replacement or additional Security Standards. The Security Standards are set out in Annex B.
"**Tigerscheme**"	shall mean a scheme for authorised penetration tests which scheme is managed by USW Commercial Services Ltd.
"**Vulnerability Scan**"	shall mean an ongoing activity to identify any potential vulnerability in any Employer Assets, the Employer's Systems Environment (or any part thereof) or the Consultant's Systems Environment (or any part thereof).

1.1 Reference to any notice to be provided by the Consultant to the Employer shall be construed as a notice to be provided by the Consultant to the Employer's Agent.

2. PRINCIPLES OF SECURITY

2.1 The Consultant shall at all times comply with the Security Policy and provide a level of security which is in accordance with the Security Policies and Standards, Good Security Practice and Law.

3. ISO/IEC 27001 COMPLIANCE AND AUDIT

3.1 The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, comply with ISO/IEC 27001 in relation to the *services* during the Call Off Contract.

3.2 The Consultant shall appoint an Information Security Manager and shall notify the Employer of the identity of the Information Security Manager on the *starting date* and, where applicable, within 5 Working Days following any change in the identity of the Information Security Manager.

3.3 The Consultant shall ensure that it operates and maintains the Information Security Management System during the *service period* and that the Information Security Management System meets the Security Policies and Standards, Good Security Practice and Law and includes:

a) a scope statement (which covers all of the Services provided under this Call Off Contract);

b) a risk assessment (which shall include any risks specific to the Services);

c) a statement of applicability;

d) a risk treatment plan; and

e) an incident management plan

in each case as specified by ISO/IEC 27001.

The Consultant shall provide the Information Security Management System to the Employer upon request within 10 Working Days from such request.

3.4 The Consultant shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within 10 Working Days after completion of the relevant audit provide any associated security audit reports to the Employer.

3.5 Notwithstanding the provisions of paragraph **Error! Reference source not found.** to paragraph **Error! Reference source not found.**, the Employer may, in its absolute discretion, notify the Consultant that it is not in compliance with the Security Policy and provide details of such non-compliance. The Consultant shall, at its own expense, undertake those actions required in order to comply with the Security Policy within one calendar month following such notification or on a date as agreed by the Parties. For the avoidance of doubt, any failure to comply with the Security Policy within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a substantial failure by the Consultant to comply with his obligations.

4. CYBER ESSENTIALS SCHEME

4.1 The Consultant shall, and shall procure that any Sub-Consultant (as applicable) shall, obtain and maintain certification to Cyber Essentials (the “Cyber Essentials Certificate”) in relation to the Services during the *service period*. The Cyber Essentials Certificate shall be provided by the Consultant to the Employer annually on the dates as agreed by the Parties.

4.2 The Consultant shall notify the Employer of any failure to obtain, or the revocation of, a Cyber Essentials Certificate within 2 Working Days of confirmation of such failure or revocation. The Consultant shall, at its own expense, undertake those actions required in order to obtain a Cyber Essentials Certificate following such failure or revocation. For the avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Certificate during the *service period* after the first date on which the Consultant was required to provide a Cyber Essentials Certificate in accordance with paragraph **Error! Reference source not found.** (regardless of whether such failure is capable of remedy) shall constitute a substantial failure by the Consultant to comply with his obligations.

5. RISK MANAGEMENT

5.1 The Consultant shall operate and maintain policies and processes for risk management (the **Risk Management Policy**) during the *service period* which includes standards and processes for the assessment of any potential risks in relation to the *services* and processes to ensure that the Security Policy is met (the **Risk Assessment**). The Consultant shall provide the Risk Management Policy to the Employer upon request within 10 Working Days of such request. The Employer may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Security Policy. The Consultant shall, at its own expense, undertake those actions required in order to implement the changes required by the Employer within one calendar month of such request or on a date as agreed by the Parties.

5.2 The Consultant shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Consultant's Systems Environment or in the threat landscape or (iii) at the request of the Employer. The Consultant shall provide the report of the Risk Assessment to the Employer, in the case of at least annual Risk Assessments, within 5 Working Days of completion of the Risk Assessment or, in the case of all other Risk Assessments, within one calendar month after completion of the Risk Assessment or on a date as agreed by the Parties. The Consultant shall notify the Employer within 5 Working Days if the Risk Profile in relation to the Services has changed materially, for example, but not limited to, from one risk rating to another risk rating.

5.3 If the Employer decides, at its absolute discretion, that any Risk Assessment does not meet the Security Policy, the Consultant shall repeat the Risk Assessment within one calendar month of such request or as agreed by the Parties.

5.4 The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, co-operate with the Employer in relation to the Employer's own risk management processes regarding the *services*.

5.5 For the avoidance of doubt, the Consultant shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this paragraph **Error! Reference source not found.**. Any failure by the Consultant to comply with any requirement of this paragraph **Error! Reference source not found.** (regardless of whether such failure is capable of remedy), shall constitute a substantial failure by the Consultant to comply with his obligations.

6. SECURITY AUDIT AND ASSURANCE

6.1 The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, complete the information security questionnaire in the format stipulated by the Employer (the "**Information Security Questionnaire**") at least annually or at the request by the Employer. The Consultant shall provide the completed Information Security Questionnaire to the Employer within one calendar month from the date of request.

6.2 The Consultant shall conduct Security Tests to assess the Information Security of the Consultant's Systems Environment and, if requested, the Employer's Systems Environment. In relation to such Security Tests, the Consultant shall appoint a third party which i) in respect of any Penetration Test, is duly accredited by CHECK, CREST (International), or Tigerscheme and, ii) in respect of any Security Test to which PCI DSS apply, is an approved scanning vendor duly accredited by the PCI. Such Security Test shall be carried out (i) at least annually, (ii) in the event of a material change in the Consultant's Systems Environment or in the Employer's System Environment or (iii) at the request of the Employer which request may include, but is not limited to, a repeat of a previous Security Test. The content, and format of any report of such Security Tests shall be approved in advance of the Security Test by the Employer. The Consultant shall provide any report of such Security Tests within one calendar month following the completion of such Security Test or on a date agreed by the Parties. The Consultant shall, at its own expense, undertake those actions required to rectify any risks identified by any Security Test in the manner and within the timeframe required by the Employer in its absolute discretion.

6.3 The Employer shall be entitled to send the Employer's Agent or such other person it shall reasonably require to witness the conduct of any Security Test. The Consultant shall provide to the Employer notice of any Security Test at least one month prior to the relevant Security Test.

6.4 Where the Consultant provides code development services to the Employer, the Consultant shall comply with the Security Policy in respect of code development within the Consultant's Systems Environment and the Employer's Systems Environment.

6.5 Where the Consultant provides software development services, the Consultant shall comply with the code development practices specified in The Statement of Requirements and Scope or in the Security Policy.

6.6 The Employer, or an agent appointed by it, may undertake Security Tests in respect of the Consultant's Systems Environment after providing advance notice to the Consultant. If any Security Test identifies any non-compliance with the Security Policy, the Consultant shall, at its own expense, undertake those actions required in order to rectify such identified non-compliance in the manner and timeframe as stipulated by the Employer at its absolute discretion. The Consultant shall provide all such co-operation and assistance in relation to any Security Test conducted by the Employer as the Employer may reasonably require.

6.7 The Employer shall schedule regular security governance review meetings which the Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, attend.

7. PCI DSS COMPLIANCE AND CERTIFICATION

7.1 Where the Consultant obtains, stores, processes or transmits payment card data, the Consultant shall comply with the PCI DSS.

7.2 The Consultant shall obtain and maintain up-to-date attestation of compliance certificates ("**AoC**") provided by a qualified security assessor accredited by the PCI and up-to-date self-assessment questionnaires ("**SAQ**") completed by a qualified security assessor or an internal security assessor, in each case accredited by the PCI (each with the content and format as stipulated by the PCI and such reports the "PCI Reports"), during the *service period*. The Consultant shall provide the respective PCI Reports to the Employer upon request within 10 Working Days of such request.

7.3 The Consultant shall notify the Employer of any failure to obtain a PCI Report or a revocation of a PCI Report within 2 Working Days of confirmation of such failure or revocation. The Consultant shall, at its own expense, undertake those actions required in order to obtain a PCI Report following such failure or revocation within one calendar month of such failure or revocation.

8. SECURITY POLICIES AND STANDARDS

8.1 The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, comply with the Security Policies and Standards set out Annex A and B.

8.2 Notwithstanding the foregoing, the Security Policy applicable to the services may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the Services. The Employer may issue instructions to the Consultant to comply with any amended Security Policy as required by the Employer, provided that where such amended Security Policy increases the burden on the Consultant pursuant to this contract, the novation shall be a compensation event. Accordingly a new clause 60.1(14) shall be added that reads "An amendment to a Security Policy pursuant to paragraph 8.2 of Contract Schedule 8 occurs which increases the burden on the Consultant pursuant to this Call Off Contract".

8.3 The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Standards.

9. CYBER SECURITY INFORMATION SHARING PARTNERSHIP

9.1 The Consultant may become a member of the Cyber Security Information Sharing Partnership in accordance with the recommendations by the NCSC during the *service period*. The Consultant may participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.

9.2 Where the Consultant becomes a member of the Cyber Security Information Sharing Partnership, it shall review the NCSC weekly threat reports on a weekly basis and implement recommendations in line with the Consultant's Risk Management Policy.

ANNEX A – EMPLOYER SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards unless specified otherwise:

a) Acceptable Use Policy

b) Information Security Policy

c) Physical Security Policy

d) Information Management Policy

e) Email Policy

f) Technical Vulnerability Management Policy

g) Remote Working Policy

h) Social Media Policy

i) Forensic Readiness Policy

j) SMS Text Policy

k) Privileged Users Security Policy

l) User Access Control Policy

m) Security Classification Policy

n) Cryptographic Key Management Policy

o) HMG Personnel Security Controls – May 2018
(published on https://www.gov.uk/government/publications/hmg-personnel-security-controls)

p) NCSC Secure Sanitisation of Storage Media
(published on https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

ANNEX B – SECURITY STANDARDS

The Security Standards are published on:
https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards:

a) SS-001 - Part 1 - Access & Authentication Controls
b) SS-001 - Part 2 - Privileged User Access Controls
c) SS-002 - PKI & Key Management
d) SS-003 - Software Development
e) SS-005 - Database Management System Security Standard
f) SS-006 - Security Boundaries
g) SS-007 - Use of Cryptography
h) SS-008 - Server Operating System
i) SS-009 - Hypervisor
j) SS-010 - Desktop Operating System
k) SS-011 - Containerisation
l) SS-012 - Protective Monitoring Standard for External Use
m) SS-013 - Firewall Security
n) SS-014 - Security Incident Management
o) SS-015 - Malware Protection
p) SS-016 - Remote Access
q) SS-017 - Mobile Devices
r) SS-018 - Network Security Design
s) SS-019 - Wireless Network
t) SS-022 - Voice & Video Communications
u) SS-023 - Cloud Computing
v) SS-025 - Virtualisation
w) SS-027 - Application Security Testing
x) SS-028 - Microservices Architecture
y) SS-029 - Securely Serving Web Content
z) SS-030 - Oracle Database
aa) SS-031 - Domain Management
bb) SS-033 - Patching

Contract Schedule 6 - Key Performance Indicators

Schedule 6 - Key Performance Indicato