



REDACTED

Introduction

NEC3 Professional Services Contract – Option G

This Delivery Agreement incorporates the NEC 3rd edition Professional Services Contract April 2013 (the **NEC3 Professional Services Contract**).

Any subsequent amendments to the NEC3 Professional Services Contract shall apply to this Model Delivery Agreement, if agreed in writing by Scape and the Partner, but shall only be incorporated into Delivery Agreements executed after such amendments are published and their inclusion has been agreed accordingly with Scape.

The following rules apply to the incorporation of clauses into a Delivery Agreement:

- a) The contract clauses are varied by the incorporation of option clauses, or a Z clause.
 - b) The option clauses defined as '**Shall apply**' in the table below will be incorporated unless otherwise agreed by the Client and Scape
 - c) The option clauses defined as '**May apply**' in the table below may apply, subject to agreement by the Client.
 - d) The Z clauses set out below shall be incorporated unless otherwise agreed in writing by the Client and Scape
 - e) The Client has sole discretion to the choice of Contract Option and Secondary options as noted above
 - f) The Client shall act as the *Employer* in this contract
 - g) The 'Client Proposed Appointment Charge' from the Framework Commercial Model is shown as the 'Employer Proposed Appointment Charge' in this agreement
 - h) The *task schedule* must include the appropriate components of the Framework Commercial Model uplifted in accordance with the Framework Agreement, e.g. using the Uplift Percentage appropriate to the forecast value of the Delivery Agreement
 - i) *staff rates* must include the appropriate rates for the Service drawn from the Framework Commercial Model and uplifted in accordance with the Framework Agreement e.g. for regional adjustment factor appropriate to the location of services delivered under the Contract and the Uplift Percentage appropriate to the forecast value of the Delivery Agreement
- Whereas:**

This Delivery Agreement is made pursuant to the Framework Agreement dated 5th January 2021 made between Scape Procure Limited and Mace Limited (the 'Framework Agreement') and incorporates those provisions of the Model Delivery Agreement set out in the Framework Agreement.

When using this Delivery Agreement, the Partner and Client (as stated in the Framework Agreement) are the parties named as 'Consultant' and 'Employer' respectively. **IT IS AGREED** as follows:

1. The **Consultant's** Obligations

The *Consultant* provides the services and complies with his obligations, acting as the *Consultant* in accordance with the *conditions of contract* set out in the Contract Data herein.

2. The **Employer's** Obligations

The *Employer* pays the amount of money and complies with its obligations in accordance with the conditions.

MAIN OPTION CLAUSES THAT SHALL APPLY:

Option Option Title

G	Priced Contract with Activity Schedule
---	--

SECONDARY OPTION CLAUSES AND ADDITIONAL OPTIONS:

Clause Option Title Applicable?

Resolving and Avoiding Disputes		
W2	Dispute resolution procedure	Shall apply
Secondary Options		
X2	Changes in the law	Shall apply
X9	Transfer of rights	
X11	Termination by the <i>Employer</i>	
X18	Limitation of liability	
X1	Price adjustment for inflation	<input checked="" type="checkbox"/> Applies if checked
X4	Parent Company Guarantee	<input type="checkbox"/> Applies if checked
X5	Sectional Completion	<input type="checkbox"/> Applies if checked
X7	Delay damages	<input type="checkbox"/> Applies if checked
X8	Collateral warranty agreements	<input type="checkbox"/> Applies if checked
X10	<i>Employer's Agent</i>	<input type="checkbox"/> Applies if checked
X12	Partnering	<input type="checkbox"/> Applies if checked
X20	Key Performance Indicators (not used with Option X12)	<input checked="" type="checkbox"/> Applies if checked
X21	Information Modelling	<input type="checkbox"/> Applies if checked
Additional Options		
13.9	Electronic Communications	<input type="checkbox"/> Applies if checked
Option Y		
Y(UK)1	Project Bank Accounts	<input type="checkbox"/> Applies if checked
Y(UK)2	The Housing Grants, Construction and Regeneration Act 1996	Shall apply
Y(UK)3	The Contracts (Rights of Third Parties) Act 1999	
Z	Additional conditions of contract	Shall apply

Contract Data and Service Information

Information provided by the Parties

The following details the Contract Data and associated Scope / Service information which is provided by the parties for this Delivery Agreement and Appended for execution.

Completion of the data in full is essential to create a complete contract.

The Main Contract Data must be completed and uploaded using ONLY the standard template provided by SCAPE.

Main Contract Data:

General Project Information,
Clauses Applicable to Main Options and Secondary options where applicable,
Data Pertaining to Optional (X) Clauses,
Y Clauses and Z Clauses where applicable.

Contract Data Provided by the Client:




Contract Data Provided by the Consultant:



Additional Contract Data provided by the parties.

One or more files may be attached in each section of the table below.

Please itemise and upload in the order you wish documents to be appended.


Ref	Item Description	Attach
	DWP Employer requirements - Real Estate Consultancy Requirements v0.5 FINAL	
	221005 Proposal to DWP for RE Advisory - ITT Submission v2	
	DWP Real Estate CG 041 Tender total	

Continues



Contract Data and Service Information

Additional Contract Data provided by the parties.
One or more files may be attached in each section of the table below.
Please itemise and upload in the order you wish documents to be appended.

Ref	Item Description	Attach
	DWP Security Policy	



Executed as a Deed

The Common Seal of / On behalf of

Department for Work and Pensions
) was hereunto affixed in the presence of / by:)



Executed as a
Deed

by Mace Limited

) REDACTED

.....
Senior Category Manager

REDACTED

.....
Full name (BLOCK CAPITALS)

Projects Commercial Lead

.....
Position/title

.....
Client Witness/Signatory

REDACTED

.....
Full name (BLOCK CAPITALS)

REDACTED

.....
Position/title

.....
Director

.....
REDACTED Full name (BLOCK CAPITALS)

.....
Position/title

.....
Company Secretary

.....
Full name (BLOCK CAPITALS)

.....
Position/title

)
)
)
on behalf of)

...
...

CONTRACT DATA FORM

Guidance: This form has been developed for use exclusively for Delivery Agreements executed using the Scape DocuSign electronic contract solution. The form is a mandatory component of the Delivery Agreement and a continuation of the Contract Data captured in the DocuSign component.

This form must be completed and uploaded at the appropriate place within the Delivery Agreement DocuSign form before execution.

If there is scope, site or service information or other documents to be appended as part of the Contract Data provided by the parties, they should be appended in the relevant order to the main DocuSign Delivery Agreement form.

PART 1A: CONTRACT DATA PROVIDED BY THE *EMPLOYER*

Completion of the data in full is essential to create a complete contract.

The following details the Contract Data which will be provided by the *Employer* for each Delivery Agreement.

Certain defined terms and information in the Contract Data will be common to all Delivery Agreements, other information included in the Contract Data will be specific to individual Projects.

When using this Delivery Agreement, the Partner (as stated in the Framework Agreement) is the party named as '*Consultant*'.

Contract data defining the following items should be documented in the main DocuSign Delivery Agreement form:

The selection of the Main Option Clauses, the selection of the
Secondary and Additional Option Clauses.

1. General

The *Employer* is:



Name

Department for Work and Pensions

Address

Finance Group
1 Hartshead Square
Sheffield
S1 2FP

Telephone

+44 300 076 6162

E-mail address

REDACTEDThe *Adjudicator* is:

Name

to be nominated by the Royal Institution of Chartered Surveyors

Address for communications

to be nominated by the Royal Institution of Chartered Surveyors

Telephone

to be nominated by the Royal Institution of Chartered Surveyors

E-mail address

to be nominated by the Royal Institution of Chartered Surveyors

The *services* are:

Department for Work and Pensions have requested that Mace provide consultancy for commision of Real Estate Advisory Services. This contract is delivery of the activities detailed within the attached Mace proposal 221005 Proposal to DWP for RE Advisory - ITT Submission v2 (Task Order .001)

The *Scope* is in:

Detailed within the attached proposal 221005 Proposal to DWP for RE Advisory - ITT Submission v2



The *language* of this contract is

English

The *law* of this contract is law of

England and Wales

The period for reply is except **2 weeks** that

The *period for retention* is **12 years** following Completion or earlier termination. (6 if underhand)

The *Adjudicator nominating body* is

the Royal Institution of Chartered Surveyors

The *tribunal* is

the Courts

The following matters will be included in the Risk Register:

UK Government changes to Covid-19 protocol or other government restrictions imposed by the UK Government in response to an epidemic or pandemic

Optional clause **13.9 Electronic communication**

does apply

2. The *Parties'* Main Responsibilities

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

access

- | | |
|-----|---|
| (1) | To people systems, sites and reports as detailed in the task orders [as per proposal] |
| (2) | Click or tap here to enter text. |
| (3) | Click or tap here to enter text. |

access date

- | |
|-------------------------------|
| Click or tap to enter a date. |
| Click or tap to enter a date. |
| Click or tap to enter a date. |

3. Time

The starting date is

05/12/2022

Monthly

The *Consultant* submits revised programmes at intervals no longer than

4. Quality

The period after the Contract Date within which the quality policy statement and quality plan programme for acceptance are provided is

2 weeks

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

0 weeks

5. Payment

The *assessment interval* is

monthly

The *currency* of the contract is the

pound sterling

The *interest rate* is

3

% per annum above the

in force

base

rate

from time to time of the

Bank of England

6. Indemnity, insurance and liability

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

EVENT	COVER	PERIOD FOLLOWING COMPLETION OF THE WHOLE OF THE SERVICES OR EARLIER TERMINATION
Liability of the <i>Consultant</i> for claims made against him arising out of his failure to use skill and care required by this contract	REDACTED in respect of each and every claim or series of claims arising out of the same original cause or source (or equivalent), without limit to the number of claims, save that there may be lower and/or annual aggregate limits of cover in respect of pollution and contamination related claims and similar where such limited cover is the norm	12 years (6 years if executed underhand)
death or bodily injury to a person (not an employee of the <i>Consultant</i>) or loss of or damage to property resulting from an action or failure to take action by the <i>Consultant</i>	REDACTED in respect of each claim, without limit to the number of claims	12 years (6 years if executed underhand)
death or bodily injury to employees of the <i>Consultant</i> arising out of and in the course of their employment in connection with this contract	The greater of the amount required by law and REDACTED in respect of each claim, without limit to the number of claims	12 years (6 years if executed underhand)

The *Employer* provides the following insurances:

- Insurance for all existing buildings and property existing within the Site or at the sole discretion of the Employer he may elect to 'self-insure' such existing buildings and property and in doing so accepts all of the Employer's associated risks arising out of or in relation to such 'self-insurance'. In accordance with an Employer's decision to 'self-insure' they do not accept any additional insurance premium/cost from the



Consultant. The Consultant is to assume the Employer insures or “self-insures” as set out above and if this is not the case the Consultant will have the opportunity to price for providing these insurances ☐ Click or tap here to enter text.

- Click or tap here to enter text. ☐ Click or tap here to enter text.

The *Consultant's* total liability to the *Employer* for all matters arising under or in connection with this contract, other than the excluded matters is limited to:

- **REDACTED** in the aggregate

Optional statements (The following optional clauses apply)

If the *Employer* has decided the completion date for the whole of the *services* The completion date for the whole of the *services* is 29/02/2024

If no programme is identified in part two of the Contract Data The period after the Contract Date within which the *Consultant* is to submit a first programme for acceptance is 4 weeks

If the <i>Employer</i> has identified work which is to meet a stated condition by a key date	The <i>key dates</i> and <i>conditions</i> to be met are	
	condition to be met	key date
	(1)	
	(2)	Please refer to 221005 Proposed Real Estate Advisory - ITT Sub
	(3)	
	(4)	Click or tap here to enter text.
	(5)	Click or tap here to enter text.

If Option Y(UK)2 is used and the final date for payment is not fourteen days after the date on The period for payment is 14 days



whic
h
pay
ment
is
due

If the
Empl
oyer
state
s
any
expe
nses

The expenses
stated by the
Employer are *Item*

Amount

Please refer to Proposal submis	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.

If Option G is used

The *Consultant* prepares forecasts of the total Time Charge expenses at intervals no longer than

4 weeks and

The *exchange rates* are those published in

on

Click or tap here to enter text.

Click or tap to enter a date.

X1 Price Adjustment for Inflation

If Option X1 is The proportions used to calculate the Price Adjustment Factor are used Applies

0.	[100 %	Linked to the index for	BCIS Labour Cost Index
0.	[Click or tap here to enter text.
0.	[Click or tap here to enter text.
0.	[Click or tap here to enter text.
0.	[Click or tap here to enter text.
0.	[Click or tap here to enter text.
		1.00 non-adjustable	Click or tap here to enter text.

The *base date* for indices is

5th January 2022

These indices are those prepared by

The Royal Institute of Chartered Surveyors
and published by the Building Cost
Information Service

X2 Changes in the Law

If Option X2 is The *law of the project* is the law of England and Wales used

X5 Sectional Completion

If Option X5 is used The *completion date* for each *section* of the *services* is N/A

section description

completion date

(1)	Click or tap here to enter text.	Click or tap to enter a date.
(2)	Click or tap here to enter text.	Click or tap to enter a date.
(3)	Click or tap here to enter text.	Click or tap to enter a date.
(4)	Click or tap here to enter text.	Click or tap to enter a date.

X7 Delay Damages

If Option X7 is used Delay damages for each *section* of the *service* are N/A with Option X5

section description

amount per day

(1)	Click or tap here to enter text.	Click or tap here to enter text.
(2)	Click or tap here to enter text.	Click or tap here to enter text.
(3)	Click or tap here to enter text.	Click or tap here to enter text.
(4)	Click or tap here to enter text.	Click or tap here to enter text.
	Click or tap here to enter text.	Click or tap here to enter text.
		N/A

The delay damages for the remainder of *service* are

X8 Collateral warranty agreements

If Option X8 is used

The *collateral warranty agreements* are:

N/A

agreement reference

third party



(1)

(2)	If requested by the Client before completion date for the who services, Mace shall provide maximum of three collateral warranties in the form of the set out in Schedule 10 of the Framework Agreement	Click or tap here to enter text.
	Click or tap here to enter text.	Click or tap here to enter text.

The forms of the collateral warranty agreements are attached to the Framework Agreement

X10 Employer’s Agent

If Option X10 is used	The <i>Employer’s Agent</i> is:	
N/A	Name	Address
	Click or tap here to enter text.	Click or tap here to enter text.
	The authority of the <i>Employer’s Agent</i> is	
	Click or tap here to enter text.	

X12 Partnering

If Option X12 is used	The <i>Client</i> is	
N/A	Name: Click or tap here to enter text.	
	Address: Click or tap here to enter text.	
	The <i>Client’s objective</i> is	
	Click or tap here to enter text.	
	The Partnering Information is in	
	Click or tap here to enter text.	



X18 Limitation of liability

If Option X18 is used	The <i>Consultant's</i> liability to the <i>Employer</i> for indirect or consequential loss for all matters other than Cladding Claims is limited to	REDACTED in the aggregate
	The <i>Consultant's</i> liability to the <i>Employer</i> for Defects that are not found until after the <i>defects date</i> is limited to	REDACTED in the aggregate

The end of liability date is **twelve (12)** years after Completion of the whole of the services. (6 for underhand)

X20 Key Performance Indicators

If Option X20 is used	The <i>incentive schedule</i> for Key Performance Indicator is in	As per the framework
	A report of performance against each Key Performance Indicator is provided at intervals of	1 months

Y(UK)1 Project Bank Account

If Option Y(UK)1 is used The *Employer* is to pay any charges made and to be paid any interest paid by the *project bank* N/A and the **Employer is to pay any charges made and is paid any interest paid by the *project bank***

Y(UK)3 The Contracts (Rights of Third Parties) Act 1999

If Y(UK)3 is used	term	<i>person or organisation</i>
	Not applicable	Click or tap here to enter text.
	Click or tap here to enter text.	Click or tap here to enter text.
If Options Y(UK)1 both used	term	<i>Person or organisation</i> and Y(UK)3 are
	Not used	Named Suppliers



The additional *conditions of contract* are identified by the amendments, alterations, additions and deletions as contained herein apply and take priority over the standard form NEC Professional Services Contract Option G

Additional Z Clauses at the request of Department For Work And Pensions ("FINAL AGREED Scape Framework Clause on Records and New Z Clause on Invoicing Requirements" word doc.)

Z28.8 The Client and the Consultant shall exchange all orders, invoices, and payments via electronic methods.

Z28.9 The following information may be required independently from the Consultant in order to verify invoices and shall be provided before or at the same time that an invoice or other claim for payment is submitted by the Consultant to the Client:

records of any Time Charge or other charge determined by reference to staff rates, including in relation to any Task Order issued under time charges and/or where applicable in respect of compensation events. Such records shall be in the form of timesheets and/or such other evidence of time spent that the Client shall reasonably require and shall be broken down according to each Task to which they relate (including details of the specific Task to which each time entry relates); the Client reserves the right to request all records required under Clause 21 of the Agreement to evidence completion of relevant activities as detailed within The Client's Statement of Requirements and Scope as requested in the Task Order issued under fixed price, and shall be sent to the person or such replacement person that the Client shall notify.

Z28.10 Option G, 52.2 is deleted and replaced with the following: "The Consultant keeps accounts and records of his Time Charge and expenses and allows the Employer or any person authorised on behalf of the Employer to inspect them at any time within working hours. The Consultant shall ensure that Subcontractors and suppliers of the Consultant agree to the same term in their appointments."

Z29 Amendments to the Secondary Option Clauses – X11 (Termination by the Client)

Z29.2 New Option X11.3: insert new option: The amount due on termination pursuant to X11.1 includes the fee percentage applied to any excess of the value of authorised and instructed Task Orders as at the date of termination over the Price for Service Provided to Date.

1. General

11.2 (2) Add further bullet point:

- provided or procured all Collateral Warranties which the *Consultant* is then obliged under this contract to provide or procure 11.2(13) At the end of the sentence add:

'Appropriately spent excludes time.'

- spent on activities included within the Commercial Inclusions Tables contained in the Pricing Procedures of the Framework Agreement,
- not justified by the *Consultant's* accounts and records,
- that should not have been paid to a Subconsultant or supplier in accordance with its contract,
- was incurred only because the *Consultant* did not
 - follow an acceptance or procurement procedure stated in the Scope,

- give an early warning which the contract required it to give or
- give notification to the *Employer* of the preparation for and conduct of an adjudication or proceedings of a tribunal between the *Consultant* and a Subcontractor or supplier and the cost of
- activities included under the Employer Proposed Appointment Charge of the Framework Agreement,
- correcting Defects after Completion,
- correcting Defects caused by the *Consultant* not complying with a constraint on how it is to Provide the Service stated in the Scope,
- for staff not used to Provide the Service (after allowing for reasonable availability and utilisation) and
- preparation for and conduct of an adjudication or proceedings of the *tribunal* between the Parties.'

11.2(26) Insert a new clause 11.2(26):

'Framework Agreement' is the framework agreement between Scape Procure Limited and the *Consultant* dated 5th January 2021.

11.2(27) Insert a new clause 11.2(27):

Framework Commercial Model as included in the Framework Agreement between Scape Procure Limited and the Consultant dated 5th January 2021.

11.2 (28) Insert a new clause 11.2(28) Data

Protection Legislation means

- i. the General Data Protection Regulation (Regulation (EU) 2016/679), the Law Enforcement Directive (Directive (EU) 2016/68) and any applicable national implementing laws as amended from time to time;
- ii. the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; and
- iii. all applicable law about the processing of personal data and privacy

11.2 (29) Insert a new clause 11.2(29)

Data Subject has the meaning given to it in the Data Protection Legislation.

11.2 (30) Insert a new clause 11.2(30)

Personal Data has the meaning given to it in the Data Protection Legislation.

11.2 (31) Insert a new clause 11.2 (31)

Cladding Claim shall mean any claim in respect of:

The combustibility of any Aluminium Composite Panels (and associated core/filler and insulation) which failed the BRE testing programme on behalf of The Department for Communities and Local Government in July and August 2017 or fails BS8414 test set out in the current Building Regulations.

12.4 Insert at the end:

'provided that Clauses 23 (Convictions), 29 (Statutory Requirements), 30 (Competition Law, Corrupt Gifts and Payments), 31 (Modern Slavery), 33 (Confidentiality and Freedom of Information), 35 (Intellectual Property) and 37.11 (Miscellaneous: Whistle Blowing) of

the Framework Agreement shall be deemed incorporated into this contract, mutatis mutandis, as if references to 'Scape' were to 'the *Employer* and references to the 'Agreement' were to 'the *contract*'.

12.5 Insert a new clause 12.5:

'A reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent re-enactment of it.'

13.9 Insert a new clause, 13.9

'The following communications shall be deemed to have no effect if made by electronic mail transmission:

- Any notification of a wish to terminate this contract or the employment of the *Consultant* under it
- Any notification by the *Consultant* of his intention to suspend performance of his obligations under this contract
- Any invoking by either party of the procedures applicable under this contract to the resolution of disputes or differences
- Any agreement between the parties amending the provisions of this contract' (*Clause 13.10 may be deleted at the Employer's sole discretion*).

14.1 Add after the final sentence:

'Notwithstanding any other provision of this contract, the terms 'acceptance', 'approval' or similar when used in the context of any acceptance or approval to be given by or on behalf of the *Employer* has the meaning 'acceptance of general principles only' and no such acceptance or approval shall diminish or relieve the *Consultant* from any of the *Consultant's* obligations or liabilities under this contract.'

19. Insert a new Clause 19:

Data Protection

Both Parties will comply with all applicable requirements of the Data Protection Legislation. These clauses are in addition to, and does not relieve, remove or replace, each Party's obligations under the Data Protection Legislation. It is agreed that:

- 19.1. Without prejudice to the generality of clause 19.1, both Parties will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of any Personal Data to each other for the duration and purposes of this agreement.
- 19.2. Without prejudice to the generality of clause 19.1, the *Consultant* shall, in relation to any Personal Data processed in connection with the performance by the *Consultant* of its obligations under this agreement:
 - 19.2.1. Process that Personal Data only on the written instructions of the *Employer* and only as required for the purpose of the performance of this agreement;
 - 19.2.2. Ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the *Employer*, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or

accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its 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 technical and organisational measures adopted by it);

- 19.2.3. Ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential;
- 19.2.4. Not transfer any Personal Data outside of the European Economic Area;
- 19.2.5. Assist the *Employer*, at the *Consultant's* cost, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
- 19.2.6. Notify the *Employer* without undue delay on becoming aware of a Personal Data breach;
- 19.2.7. At the written direction of the *Employer*, delete or return Personal Data and copies thereof to the *Employer* on termination of the agreement; and
- 19.2.8. Maintain complete and accurate records and information to demonstrate its compliance with this clause and allow for audits by the *Employer* or the *Employer's* designated auditor.
- 19.3. The *Employer* does not consent to the *Consultant* appointing any third-party processor of Personal Data under this agreement.

2. The Parties' main responsibilities

21. Amend as follows:
 - 21.2 Delete and replace with:

'The *Consultant's* obligation is to use (and warrant that it has used) all the reasonable skill, care and diligence normally used by competent and appropriately qualified professionals experienced in providing services similar to the *service*.'
 - 21.5 Insert a new Clause 21.5:

'The *Consultant* checks the Scope provided by the *Employer* and satisfies itself that its own provision of the *service*, including any proposals, designs and Scope or specification documents for a subsequent construction contract meet the *Employer's* Scope with no discrepancy. Where there is ambiguity, inconsistency or conflict between these documents the *Employer's* Scope will prevail'.
 - 21.6 Insert a new clause 21.6:

'The *Consultant* performs the Service in accordance with relevant laws and regulations, statutory and other requirements ('Laws') and (to the extent that the *Consultant* can control the same) such that the product of the Service complies with all relevant Laws.'
- 24.5 Insert a new Clause 24.5:

'The *Consultant*, in relation to any subletting of any portion of the service:

 - Procures that the relevant subcontract contains such obligations as necessary to ensure that it is in all respects compatible with the terms of this contract and, without limitation, steps down the obligation to use the degree of skill, care and diligence specified in this contract and that requires collateral warranties in favour of the

Employer to be provided in the forms specified in the Framework Agreement and with any amendments as permitted by the Framework Agreement.

- Procures that all relevant subcontracts shall be executed and delivered as a deed
- Warrants each Subcontractor's compliance with this contract's Modern Slavery Act requirements
- Warrants that all Subcontractors are fully aware of their obligations under the CDM Regulations and are fully competent and are adequately resourced to meet those obligations
- Provides to the *Employer* a certified copy of any subcontract (save for particulars of the cost of such subcontract service unless other provisions of this contract or the Framework Agreement oblige the *Consultant* to disclose them)

The *Consultant* does not appoint a subcontractor if there are compulsory grounds for excluding the subcontractor under regulation 57 of the Public Contracts Regulations 2015.' 24.6 Insert a new clause, 24.6

'The *Consultant* includes in any subcontract awarded by him provisions requiring that:

- payment due to the Subcontractor under the subcontract is made no later than 30 days after receipt of a valid and undisputed invoice unless the Framework Agreement required the *Consultant* to make earlier payment to the Subcontractor
- Invoices for payment submitted by the Subcontractor are considered and verified by the *Consultant* in a timely fashion
- Undue delay in considering and verifying invoices is not sufficient justification for falling to regard an invoice as valid and undisputed, and
- Any contract awarded by the Subcontractor for work included in this contract includes provisions to the same effect as these provisions.'

26 Add a new clause 26 as follows:

'The *Consultant* shall enter a novation agreement in the form specified in the Framework Agreement with the *Employer's* contractor within 14 days of being asked to do so in writing and shall, within 14 days of being provided with an engrossment, execute and return to the *Employer* the *collateral warranty agreement* in favour of the *Employer*, but with such amendments as the *Consultant*, *Employer* and *Employer's* contractor may agree, such agreement not to be unreasonably withheld or delayed.'

5. Payment

50.3 Insert at the end of the second bullet point:

'less expenses included in the Commercial Inclusions Tables from the Framework Agreement's Pricing Procedures,'

51.6 Insert a new clause as follows:

'In addition to any other legal rights and remedies of the *Employer*, whenever any sum of money is recoverable from or payable by the *Consultant* under this contract that sum may be deducted from any sum then due, or which at any time thereafter becomes due to the *Consultant* under this contract provided that the *Employer* notifies the *Consultant* in writing not later than three days before the final date for payment of the amount to be paid and the basis on which it is calculated.'

6. Compensation Events

63.10

At the end of the sentence add:

'Rates for subconsultant staff are calculated by applying the *Uplift Percentage* to the subconsultant's proposed rate. Unless the *Employer* otherwise agrees, proposed rates must not exceed the relevant regionally adjusted People Rates for the applicable role and seniority stated in the relevant table of the Framework Commercial Model. If the *Employer* and *Consultant* do not agree on the rate to be used, the *Employer* assesses the rate based on the *staff rates*. The agreed or assessed rate becomes the *staff rate* for that designation of person.'

63.19

Insert a new clause as follows:

The *Employer* and *Consultant* may agree rates or lump sums to assess the change to Prices or Prices for new items in the Task price list. If the *Employer* and *Consultant* do not agree on the rate or lump sum to be used, the *Employer* assesses the rate or lump sum based on the *staff rates*.

8. Indemnity insurance and liability

81.1

Amend the insurance table:

delete the words 'and care normally used by professionals' in the first insurance of the Insurance Table and replace with:

', care and diligence normally used by competent and appropriately qualified professionals experienced in'

83

Insert a new Clause 83:

83.1 Before the *starting date* and on each renewal of the insurance policy until the *defects date*, the *Consultant* submits to the *Employer* for acceptance certificates which state that the insurance required by the contract is in force. After the *defects date* and on each renewal of the insurance policy until the end of the periods stated in the Contract Data for which insurance is to be maintained, the *Consultant* submits to the *Employer* for acceptance certificates which state that insurance required by this contract is in force.

The certificates are signed by the *Consultant's* insurer or insurance broker. The *Employer* accepts the policies and certificates if the insurance complies with the contract and if the insurer's commercial position is strong enough to carry the insured liabilities. The *Employer's* acceptance of an insurance certificate provided by the *Consultant* does not change the responsibility of *Consultant* to provide the insurances stated in the Contract Data.

83.2 The Parties comply with the terms and conditions of the insurance policies which they are a Party.

84

Insert a new Clause 84:

If the *Consultant* does not provide insurance

84.1

The *Employer* may insure an event or liability which the contract requires the *Consultant* to insure if the *Consultant* does not submit a required certificate. The cost of this insurance to the *Employer* is paid by the *Consultant*.

85 Insert a new Clause 85:

Insurance by the *Employer*

- 85.1 The *Employer* submits certificates for insurance provided by the *Employer* to the *Consultant* for acceptance before the *starting date* and afterwards as the *Consultant* instructs. The *Consultant* accepts the certificates if the insurance complies with the contract and if the insurer's commercial position is strong enough to carry the insured liabilities.
- 85.2 The *Consultant's* acceptance of an insurance certificate provided by the *Employer* does not change the responsibility of *Employer* to provide the insurances stated in the Contract Data.
- 85.3 The *Consultant* may insure an event or liability which the contract requires the *Employer* to insure if the *Employer* does not submit a required certificate. The cost of this insurance to the *Consultant* is paid by the *Employer*.

9. Termination

90.5 Insert the following new clause: 90.5

'The Public Contracts Regulations 2015

- 90.5 The *Employer* may terminate the *Consultant's* obligation to Provide the Service if any of the provisions of regulation 73(1) of The Public Contracts Regulations 2015 apply.
- The *Employer* may terminate the *Consultant's* obligation to Provide the Services if any of the provisions of paragraph 73(1) of The Public Contracts Regulations 2015 apply.
- If the *Employer* terminates under the provisions of paragraph 73(1)(b) of the Public Contracts Regulations 2015 as a result of information not disclosed by the *Consultant* at the Contract Date, the procedures and amounts due on termination are the same as if the *Consultant* has substantially failed to comply with his obligations.
- If the *Employer* otherwise terminates under the provisions of paragraph 73(1) of the Public Contracts Regulations 2015, the procedures and amounts due on termination are the same as if the Employer no longer requires the services.
- 90.6 The *Consultant* does not appoint a Subconsultant or supplier if there are compulsory grounds for excluding the Subconsultant or supplier under regulation 57 of the Public Contracts Regulations 2015.
- 90.7 The *Consultant* includes in any subcontract awarded by him provisions requiring that
- payment due to the Subconsultant or supplier under the subcontract is made no later than 30 days after receipt of a valid and undisputed invoice, unless this contract requires the *Consultant* to make earlier payment to the Subconsultant or supplier,
 - invoices for payment submitted by the Subconsultant or supplier are considered and verified by the *Consultant* in a timely fashion, undue delay in considering and verifying invoices is not sufficient justification for failing to regard an invoice as valid and undisputed and
 - any contract awarded by the Subconsultant or supplier for work included in this contract includes provisions to the same effect as these provisions

X4 Parent Company Guarantee

Delete "Scope" in line 3 and insert "Framework Agreement Schedule 5" N/A

X7 Delay Damages

X7.1 The clause is deleted and replaced by the following.

'The Consultant pays delay damages at the rate stated in the Contract Data for each day from the Completion Date until the earlier of

- Completion and
- The date on which the Employer issues a termination certificate.'

Option Y(UK)1: PROJECT BANK ACCOUNT

The secondary Option is deleted and replaced with

Defined terms

Y1.1

(1) Joining Deed is an agreement in the form set out in the contract under which the Supplier joins the Trust Deed.

(2) Named Suppliers are named suppliers and other Suppliers who have signed the Joining Deed.

(3) The Payment Schedule is a list of payments to be made to the Consultant and Named Suppliers from the

Project Bank Account.

(4) Project Bank Account is the account used to receive payments from the Employer and the Consultant and to make payments to the Consultant and Named Suppliers.

(5) Project Bank Account Tracker is a register of all payments made to and from the Project Bank Account and the date each payment was made and is in the form stated in the Scope.

(6) A Supplier is a person or organisation who has a contract to

- provide a service or
- provide a service to Provide the Service.

(7) Trust Deed is an agreement in the form set out in the contract which contains provisions for administering the Project Bank Account.

Project Bank Account

Y1.2 The account holder establishes the Project Bank Account with the project bank within eight weeks of the

Contract Date.



Y1.3 Unless stated otherwise in the Contract Data, the Consultant pays any charges made and is paid any

interest paid by the project bank. The charges and interest by the project bank are not included in the assessment of the amount due.

Y1.4 If the account holder is the Consultant, it submits to the Employer for acceptance details of the banking

arrangements for the Project Bank Account. A reason for not accepting the banking arrangements is that

they do not provide for payments and inspections to be made in accordance with the contract. The

Consultant provides to the Employer copies of communications with the project bank in connection with the

Project Bank Account.

Named Suppliers

Y1.5 The Consultant includes in its contracts with Named Suppliers the arrangements in the contract for the

operation of the Project Bank Account and Trust Deed. The Consultant informs the Named Suppliers it

appoints, the details of the Project Bank Account and the arrangements for payment of amounts due under their contracts.

Y1.6 The Consultant submits proposals for adding a Supplier to the Named Suppliers to the Project Manager for

acceptance. A submission includes the Suppliers stated in the Scope and other Suppliers requested by the

Contractor. A reason for not accepting a submission is that the addition of a Supplier does not comply with

the Scope. The Employer, the Consultant and the Supplier sign the Joining Deed after acceptance.

Payments

Y1.7 Until the Project Bank Account is established, payment is made by the Employer to the Consultant.

Y1.8 The Consultant shows in the application for payment the amounts due to Named Suppliers in accordance with their contracts.



- Y1.9 Within the time set out in the banking arrangements to allow the project bank to make payment to the Consultant and Named Suppliers in accordance with the contract, the Consultant prepares
- ☐ the Payment Schedule, provides a copy to the Employer and provides the information in the Payment Schedule to the project bank,
 - ☐ the Employer makes payment to the Project Bank Account of the amount which is due to be paid under the contract and
 - ☐ the Consultant makes payment to the Project Bank Account of any amount which the Employer has informed the Consultant it intends to withhold from the certified amount and which is required to make payment to Named Suppliers.
- Y1.10 The Consultant notifies the Employer if the amount due to any Named Supplier stated in the Payment Schedule is different from that in the payment certificate and provides reasons for the change.
- Y1.11 If the account holder is the Consultant, it authorises payment in accordance with the Payment Schedule no later than one day before the final date for payment. Following payment, the Employer checks the amounts paid to the Named Suppliers by inspecting the Project Bank Account.
- Y1.12 If the account holder is the Parties, they jointly authorise payment in accordance with the Payment Schedule no later than one day before the final date for payment.
- Y1.13 Following authorisation, the Consultant and Named Suppliers receive payment from the Project Bank Account of the sums set out in the Payment Schedule as soon as practicable after the Project Bank Account receives payment.
- Y1.14 The Consultant updates the Project Bank Account Tracker and submits it to the Employer within one week of any payment being made from the Project Bank Account.
- Y1.15 A payment which is due from the Consultant to the Employer is not made through the Project Bank Account.

Effect of Payment

- Y1.16 Payments made from the Project Bank Account are treated as payments from the Employer to the Consultant in accordance with the contract. A delay in payment due to a failure of the



Consultant to comply with the requirements of this clause is not treated as late payment under the contract.

Trust Deed

Y1.17 The Employer, the Consultant and named suppliers sign the Trust Deed within two weeks of the Contract Date.

Termination

Y1.18 If the Employer issues a termination certificate, no further payment is made into the Project Bank Account.

Y(UK)2: Housing Grants, Construction and Regeneration Act 1996

Y2.2, delete clause and replace with the following.

The date on which a payment becomes due is the later of the date of receipt by the Party

☐ making payment of an invoice, issued in accordance with

these conditions of contract and

☐ fourteen days after the assessment date.

The date on which the final payment becomes due is the later of the date of receipt by the

☐ Party making payment of an invoice, issued in accordance with

these conditions of contract and

o if the Employer makes an assessment after the defects date or the date the last Defect is corrected, six weeks after the defects date or the date the last Defect is corrected, whichever is the later,

o if the Employer does not make an assessment after the defects date or the date the last Defect is corrected, two weeks after the Consultant issues its assessment or

o if the Employer has issued a termination certificate, fifteen weeks after the issue of the certificate.

The final date for payment is seven days after the date on which payment becomes due, or a different period for payment if stated in the Contract Data.

X21 Information Modelling

Insert new Option X21: Information Modelling N/A

Defined terms

21.1 (1) The Information Execution Plan is the *information execution plan* or is the latest Information Execution Plan accepted by the *Employer*. The latest Information Execution Plan accepted by the *Employer* supersedes the previous Information Execution Plan.

(2) Project Information is information provided by the *Consultant* which is used to create or change the Information Model.

(3) The Information Model is the electronic integration of Project Information and similar information provided by the *Employer* and other Information Providers and is in the form stated in the Information Model Requirements.

(4) The Information Model Requirements are the requirements identified in the Scope for creating or changing the Information Model.

(5) Information Providers are the people or organisations who contribute to the Information Model and are identified in the Information Model Requirements.

Collaboration

X21.2 The *Consultant* collaborates with other Information Providers as stated in the Information Model Requirements.

Early Warning

X21.3 The *Consultant* and the *Employer* give an early warning by notifying the other as soon as either becomes aware of any matter which could adversely affect the creation or use of the Information Model.

Information execution plan

X21.4 (1) If an Information Execution Plan is not identified in the Contract Data, the *Consultant* submits a first Information Execution Plan to the *Employer* for acceptance within the period stated in the Contract Data.

(2) Within two weeks of the *Consultant* submitting an Information Execution Plan for acceptance, the *Employer* notifies the *Consultant* of the acceptance of the Information Execution Plan or the reasons for not accepting it. A reason for not accepting an Information Execution Plan is that it does not comply with the Information Model Requirements or it does not allow the *Consultant* to Provide the Service.

If the *Employer* does not notify acceptance or non-acceptance within the time allowed, the *Consultant* may notify the *Employer* of that failure. If the failure continues for a further one week after the *Consultant's* notification, it is treated as acceptance by the *Employer* of the Information Execution Plan.

(3) The *Consultant* submits a revised Information Execution Plan to the *Employer* for acceptance within the period for reply after the *Employer* has instructed it to and when the *Consultant* chooses to.

(4) The *Consultant* provides the Project Information in the form stated in the Information Model Requirements and in accordance with the accepted Information Execution Plan.

Compensation Events

X21.5 If the Information Execution Plan is altered by a compensation event, the *Consultant* includes the alterations to the Information Execution Plan in the quotation for the compensation event.

Use of information model

X21.6 The *Employer* owns the Information Model and the *Consultant's* rights over Project Information except as stated otherwise in the Information Model Requirements. The *Consultant* obtains from a Subcontractor equivalent rights for the *Employer* over information prepared by the Subcontractor. The *Consultant* provides to the *Employer* the documents which transfer these rights to the *Employer*.

Liability



X21.7 (1) The following are *Employer* 's liabilities.

☐ A fault or error in the Information Model other than a Defect in the Project Information. ☐ A fault in information provided by Information Providers other than the *Consultant*.

(2) The *Consultant* is not liable for a fault or error in the Project Information unless it failed to provide the Project Information using the skill care and diligence normally used by competent and appropriately qualified professionals, experienced in providing information similar to the Project Information.



PART 2A: CONTRACT DATA PROVIDED BY THE CONSULTANT

Completion of the data in full is essential to create a complete contract.

1. General

The *Consultant* is:

Name	Mace Limited
Address for communication	155 Moorgate London EC2M 6X
Telephone	020 3322 3000
E-mail address	REDACTED

The key people are

(1) Name	REDACTED
Job	Associate Director
Responsibilities	Click or tap here to enter text.
Qualifications	Click or tap here to enter text.
Experience	Click or tap here to enter text.
(2) Name	Click or tap here to enter text.
Job	Please refer to proposal or Task order
Responsibilities	Click or tap here to enter text.
Qualifications	Click or tap here to enter text.
Experience	Click or tap here to enter text.

The *staff rates* are:

name/designation

rate ***

See attached Rate Card within Section of the attached proposal DWP RE Advisory V2

See attached proposal for Rate Card, Forecast & Resource Plan for full breakdown



Click or tap here to enter text.
Click or tap here to enter text.
Click or tap here to enter text.

Click or tap here to enter text.
Click or tap here to enter text.
Click or tap here to enter text.

***[Unless the *Employer* agrees the charge must not exceed the equivalent, annually adjusted ‘People Rate with expenses’ from the Framework Commercial Model after adjustment for geographic location and appropriate Uplift Percentage.]

The following matters will be included in the Risk Register

Click or tap here to enter text.

Optional Statements

If the <i>Consultant</i> is to decide the <i>completion date</i> for the whole of the <i>services</i>	The <i>completion date</i> for the whole of the <i>services</i> is	29/02/2024
---	--	------------

If a programme is identified in the Contract Data	The programme is	Click or tap here to enter text.	identified in the Contract Data is
---	------------------	----------------------------------	------------------------------------

If the <i>Consultant</i> states any expenses	The <i>expenses</i> stated by the <i>Consultant</i> are	<table><thead><tr><th>Item</th><th>amount</th></tr></thead><tbody><tr><td>All expenses identified in the Method of Operation**</td><td>NIL ***</td></tr><tr><td>All expenses identified in the Framework Agreement’s Pricing Procedures**</td><td>NIL ***</td></tr><tr><td>Additional expenses and disbursements not included in the Commercial Inclusions Table of the Framework Agreement Pricing Procedures</td><td>Click or tap here to enter text.</td></tr><tr><td>Click or tap here to enter text.</td><td>Click or tap here to enter text.</td></tr></tbody></table>	Item	amount	All expenses identified in the Method of Operation**	NIL ***	All expenses identified in the Framework Agreement’s Pricing Procedures**	NIL ***	Additional expenses and disbursements not included in the Commercial Inclusions Table of the Framework Agreement Pricing Procedures	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Item	amount											
All expenses identified in the Method of Operation**	NIL ***											
All expenses identified in the Framework Agreement’s Pricing Procedures**	NIL ***											
Additional expenses and disbursements not included in the Commercial Inclusions Table of the Framework Agreement Pricing Procedures	Click or tap here to enter text.											
Click or tap here to enter text.	Click or tap here to enter text.											

**[No expenses are to be included for Prime Core or Core Services covered as defined in the Framework Agreement and included in the Charges and Uplift Percentages within the Framework Commercial Model.]

If the <i>Consultant</i> requires additional access	The <i>Employer</i> provides access to the following persons, places and things	<table><thead><tr><th>access to</th><th>access date</th></tr></thead><tbody><tr><td>Click or tap here to enter text.</td><td>Click or tap to enter a date.</td></tr><tr><td>Click or tap here to enter text.</td><td>Click or tap to enter a date.</td></tr><tr><td>Click or tap here to enter text.</td><td>Click or tap to enter a date.</td></tr></tbody></table>	access to	access date	Click or tap here to enter text.	Click or tap to enter a date.	Click or tap here to enter text.	Click or tap to enter a date.	Click or tap here to enter text.	Click or tap to enter a date.
access to	access date									
Click or tap here to enter text.	Click or tap to enter a date.									
Click or tap here to enter text.	Click or tap to enter a date.									
Click or tap here to enter text.	Click or tap to enter a date.									



If Option G is used

The *task schedule* is

Task .001 - 221005
Proposal to DWP for

RE Advisory - ITT

Submission v2

Employer Proposed Appointment Charge to be used in
the *task schedule* is

£n/a***

The *Uplift Percentage* is

REDACTED

**[Must not exceed the rate stated with he Framework Commercial Model.]

Z4 .0 Information Modelling

N/A

If Option Z4.0 is used

If no Information Execution Plan is identified in part two of the Contract Data	The period after that Contract Date within which the Consultant is to submit a first Information Execution Plan for acceptance is:	Click or tap here to enter text.
---	--	----------------------------------

Y(UK)1 Project Bank Account

If Option Y(UK)1 is used	The <i>project bank</i> is
	Not used
	<i>named suppliers</i> are
	Click or tap here to enter text.



Employer Requirements

Provision of Real Estate Advisory Services for DWP Front of House Estate

Contract Schedule 1 - The Statement of Requirements and Scope

1. Background to the Employer

The Department for Work and Pensions (the Employer) is responsible for welfare, pensions and child maintenance policy. As the UK's biggest public service department it administers the State Pension and a range of working age, disability and ill health benefits to around 20 million claimants and customers. The Employer delivers these services across England, Wales and Scotland.

Labour Market intervention services: Job centres

A principal focus for DWP is supporting people back into work, and into better jobs. This is undertaken through our extensive national job centre network, which is currently (including c 150 opened on a short term basis during the pandemic) c800 across the UK.

We will divest short term job centre sites in the next few years, and in the current spending review period to March 2025, are undertaking a small number of further network changes.

Health & Disability Services

The principal health & disability benefits are managed through the following arrangements:

- The HDAS contract (Health & Disability Assessment Service) delivers work capability assessments (WCAs) on behalf of DWP. The Centre for Health and Disability Assessments (CHDA) are the current contracted supplier to deliver the Work Capability Assessment (WCA) and assessments for other non-WCA benefits including the Industrial Injuries Benefits and Veterans UK assessments.

- Personal Independence Payments (PIP)- PIP Health Contracts are delivered by two Assessment Providers; Independent Assessment Services (IAS) and Capita. These organisations carry out the functional assessment to enable the DWP decisions makers to award (or not award) PIP.

Current Estate

These services are predominately delivered from publicly accessible health assessment centres across the UK, on the following basis:

WCA/HDAS Estate – These services are delivered by CHDA from c111 DWP sites, predominately customer facing assessment centres, and CHDA run back office/contact centre functions. Most sites have lease breaks in 2023, and lease expiries in 2028.

PIP Estate – these are delivered from c182 supplier held sites, with costs charged back to DWP. These are a mix of leases, licences, short term hire agreements. Most leases are being renewed to 2028 with breaks in 2023 and 2025.

Health Transformation Programme

The Health Transformation Programme (HTP) is in the process of transforming the delivery of health and disability services via delivery of a single Functional Assessment Service (FAS) supported by a single digital platform developed by DWP.

An Invitation to Tender was issued in the Autumn 2021 for new Health service contracts effective July 2023-28. This will award 5 lots (one out of scope for estates in NI) in the UK.

Current Contract Structure - to July 2023		
Service	Work Capability Assessments (WCA)	PIP (<u>Personal</u> Independence Payments)
Supplier	CHDA	IAS and Capita
Geography/Lots	National (GB and NI)	National (3 Regional Lots)
Estate Platform	Mainly DWP - stand alone and collocated sites. 9 sites via CHDA	Supplier provided



2023-2028 Contracts		
Service	Work Capability Assessments (WCA)	PIP (Personal Independence Payments)
Geography/Lots	5 Regional Lots with Suppliers delivering both services (PIP out of scope for Scotland)	
Estate Platform	Mainly DWP - stand alone and collocated sites.	Supplier provided

FAS Contract – The HTP Programme Board approved in February 2021 the retention of the health assessment estates ‘status quo’:

- DWP will continue to provide estate throughout the UK as we currently do as part of the HDAS (WCA delivery) contract (c45%).
- Suppliers will provide all other estate, required to deliver PIP assessments (Scotland out of scope from August 2023). This could be leased directly, sub-leased or casual hire etc.

HTP have supported the production of the service requirements for the 2023 - 2028 FAS contract which was published on 12 November 2021.

Health Transformation Area (HTA)

In parallel with the launch of new service contracts, the Health Transformation Programme plan to pilot a new approach to integrating services by creating a Departmental Transformation Area (DTA) to develop the new service on a small scale in several sites. Lessons learnt from DTA will be rolled out during contract or from 2028 onwards

The HTA provides an environment for HTP to build, prove and scale the new Health Assessment Service (HAS) for all claimants who require a health assessment. This provides a safe environment to iterate and learn about services, systems and effects on users in a controlled environment. In particular:

- Provide learning to inform the transition and implementation approach to migrate from existing services to the Single Service.
- Provide an area to support the development of policy and Green Paper proposals.
- Provide an opportunity to explore and broaden our role in engaging claimants in work-related support.

Phase 1 went live in April 2021 in a London site with a second Phase1 DTA site in Birmingham late October/early November 2021. This is being further rolled out in 2023.

HTP Estates Strategy

Although there is not an intention to make significant change to the estate at the start of the new contracts, it is envisaged that there will be efficiency- reductions in the estate footprint by 2028 – via time efficiencies, channel shift, service transformation. However, there will be limited opportunities to make efficiencies in the early part of the FAS contract until learning and evaluation of efficiencies can be completed.

The Employer operates an 'Estates Target Operating Model' (**ETOM**), which is described further in Annex 1.

2. The Employer's Requirements

There are two elements to the commission

Health Transformation Estate Advisory/ Liaison

to be the principal Estates liaison with the Health Transformation Programme.

The proposed commission would provide continued real estate support for the Programme to provide high level strategic estates advice into the programme and ongoing due diligence covering both novation of existing supplier leases across DWP and the acquisition of a new property as the contingency option.

FAS 2023 – 2028 (through to 28 February 2024)

Provide real estate expertise to the Programme to develop and monitor the progress through to the successful transition of the Service to the New Suppliers on 28 February 2024.

- Liaison with DWP Legal on accompanying contract schedules for Estates
- Liaison with Transition work stream on estates impacts during transition
- Identifying requirements for wider estate services such as transactional (eg lease assignment) and liaising per agreed protocols to involve those estate functions
- Provide expert real estate support for Supplier Q & As, Dialogue and evaluation phases.
- Review and involve as required wider estate support co-ordinate the validation of estates data collation data room refreshes if required for any change to tender activity
- Provide high level estate cost modelling and, involving as required wider estate support for Estate Financial Cost breakdown e.g. Set up costs, Dilapidations.
- Miscellaneous Estates support & response to Programme requirements and priorities

HTA (activity likely to run through to February 2024)

- Liaison with/advice to HTA on strategy following engagement with Suppliers on HTA proposals
- Identifying requirement and supporting initial stages of mobilising DWP Estates activity on PIP site novation's, e.g. risk assessments, capacity assessments, transaction management and due diligence, site alterations, business case. Ongoing management of this activity is not anticipated to be part of this current requirement.
- Liaison in respect of co-ordinating DWP Estate's input into new site acquisition (if required as contingency option) – start in Sept 2021.
- Liaison on bringing in relevant DWP's estates teams in respect of potential reconfiguration work to existing CHDA sites e.g. reducing number of assessment rooms to create a communal space for co-location to take place
- Provide initial advice/guidance on any emerging estate management issues & identifying the need for internal estates team involvement

Job Centre Transformation Advisory/ Strategic Consultancy

This involves 2 elements:

(a) Site specific Estate Footprint change Project advisory support

A small proportion of time on a reactive and as required basis supporting estate planning for changes to the job centre network: Activities include, but not limited to:

- Driving completion of estate feasibility for potential estate change projects by site level estate planning levels, to required deadlines & milestones
- Being a point of escalation and supporting the resolution of blockers, keeping the Employer & National FOH Planning Lead informed and aware by exception of risks to delivery & support with recommendations to resolve
- mentoring and supporting internal DWP Estate Planning Leads in working up site level estate change business cases for job centre network changes,
- potentially presenting some of these business cases to the relevant Governance Boards

□

(b) Strategic portfolio modelling

- Work in collaboration with internal DWP Estates teams, to gather from existing DWP sources key business intelligence to facilitate options analysis for properties across the portfolio
- Provide strategic estate modelling & portfolio option analysis for job centre network change
- Support initial mobilisation/ resource assessment for change activity arising from this.

Operating approach

This commission will report into the DWP FOH Estate Planning Lead, within the in-house Estates Strategy, Portfolio & Leasehold function with other interactions as agreed. That wider team is also supported by leasehold & Landlord Management Suppliers, who are currently Cushman & Wakefield for real estate services, and Dentons for legal services. This role will

have no day to day over-sight or management of these suppliers, but may interact with them for input into estate planning from time to time.

By agreement and for resilience purposes, elements of activity (especially around progress updates) may involve the Mace team over-lapping/ duplicating to provide a shared understanding of key activity.

Inspection of any sites is likely to be exceptional. This role may require occasional attendance at face to face meeting on one of DWP's 7 corporate sites (excluding Scotland sites), but will predominately be remote, via DWP's Teams platform.

3. Resource Requirements

The Department currently envisage that this requirement would equate to more than a single FTE. However, as there maybe a requirement to flex up or down to meet the requirements of the Programme, we welcome the Supplier's views on how you might deliver this and with what resource.

Required qualifications / experience:

- Not less than 5 years (& ideally not less than 10 years) corporate real estate advisory experience.
- Membership of the Royal Institution of Chartered Surveyors
- A strong team ethic is essential, allied to an ability to communicate clearly and effectively with a wide and diverse stakeholder community.
- Support/ coaching skills as necessary in the development of business cases
- Experience of working with central government departments desirable
- Must be able to quickly establish an understanding of the Employer's organisational environment

Consultant Personnel Requirements

The Employer requires that all Consultant Personnel employed, whether permanent or temporary, on the provision of the services are subject to the requirements of the HM Government Baseline Personnel Security Standard (BPSS).

There is no requirement to apply to the Employer or any other third party for BPSS clearance. BPSS clearance is obtained if the following steps have been completed as part of your organisation's pre-employment checks:

- Verification of identity
- Verification of Nationality and Immigration Status (including an entitlement to undertake the work in question)
- Verification of Employment history (past 3 years)
- Verification of Criminal record (unspent convictions only). This will require a basic disclosure certificate (at cost via Disclosure and Barring Service, Disclosure Scotland and Access Northern Ireland).

Copies of the current HM Government Baseline Personnel Security Standard, providing further information regarding how each of these steps should be verified, can be found via the

following link [Government Baseline Personnel Security Standard](#). The Consultant is expected to arrange the BPSS checks at no additional charge.

All Consultant Personnel must comply with the Employer's Security Policy. The Consultant will only be expected to comply with those Security Policies and Standards that are applicable to their delivery model and technologies used.

The Consultant must be able to immediately (on contract award) resource this requirement with Personnel meeting the requirements above).

4. Proposal

- Please provide confirmation of availability onto the timescale requested
- Details of the key personnel proposed to be used in delivering the required services, including rationale for their appointment.
- A detailed commercial breakdown to be based on the following:
 - Fee proposal for carrying out the defined duties as detailed in the final agreed scope, including a detailed activity schedule with day/hourly rates
 - Ad-hoc services:
 - Day rates for different staff grades
 - Hourly rates for different staff grades

Annex 1 - The Client's 'Estates Target Operating Model' (ETOM)

Within the Department, the Client's People, Capability and Place Directorate are accountable for the delivery of all aspects of real estate services, supported by the Estates Category Management Team within Commercial Directorate to undertake all commercial activity required within the complex estates portfolio.

The Client operates an 'Estates Target Operating Model' (ETOM), shown in Figure 1, whereby a large proportion of the estates management is out-sourced to an independent third party organisation ('the Supply Chain Integrator'). The Supply Chain Integrator is independent from the Client's Supply Chain and provides an aggregated data, reporting and systems service. As of 1st May 2022, the Client's Supply Chain Integrator KBR is responsible for:

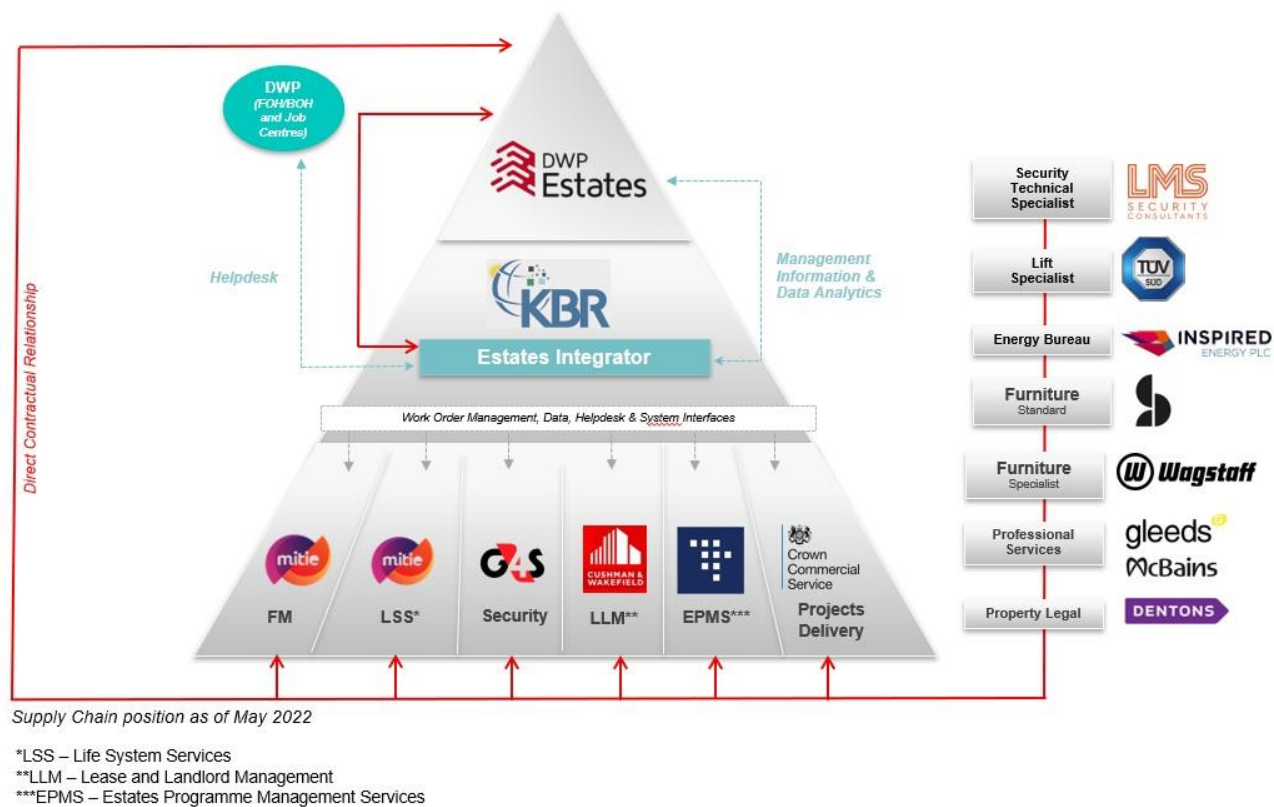
- a) providing a single up-to-date and accurate version of all Client data and information, including a master asset register;
- b) reporting holistically across the Client's estate and estate services;
- c) processing all supply chain invoices for payment;
- d) providing a help desk to the Client's workforce for all estates related problems, incidents or maintenance; and
- e) providing a CAFM system and process for the creation, dissemination, management and closure of work orders between the Client and members of the Client's supply chain.

The estate strategy planning role in the model, which this commission will support, supports the Department with strategic estate planning, and within the estates model, is responsible for estate planning upto business case approval, for estate change, such as re-locating, divesting

or re-sizing sites, and ensuring capacity for headcount demand. It then transfers responsibility to Estate Project Deliver, supporting as required. The Client's Estate project delivery function is also supported by a new Estates Programme Management Service (EPMS) delivered by Turner & Townsend Project Management Limited (Turner & Townsend), which went live on 1st February 2022. Turner & Townsend will provide robust management and oversight across all types of projects for the Client's estate. They will be responsible for setting governance, providing robust Management Information, and oversee cost and risk management for the Client's project pipeline, including major and minor Capex projects, lifecycle works (LCW) and other strategic change programmes.

Turner & Townsend will work closely with the Client's construction professional services suppliers, listed in Table 3, project delivery suppliers and other supply chain members to ensure all project works are initiated, managed and delivered to high standards providing overall value for money, and in line with the Client's strategy and vision.

Figure 1: The Client's Estates Target Operating Model (ETOM)



ETOM Suppliers

Suppliers listed within Figure 1 are referred to by the Client as 'towers:'

- **FM (Facilities Management):** This tower includes the FM and LSS contracts, supplied by Mitie FM Ltd, the Client's Energy Bureau provided by Inspired Energy Plc and furniture, fittings and equipment (FFE) contracts, supplied by Southern's Broadstock Ltd and Wagstaff Interiors Group;
- **Security:** The security tower consists of several contracts for physical security guards and systems, supplied by G4S (SS) UK (G4S);
- **Projects Delivery:** This includes the providers of construction professional services listed in Table 3, as well as all providers of construction, fit-out and Lifecycle Works currently appointed on the Client's soon to expire 'Estate Jobcentre & Office Fit Out Contractor Framework,' shown in Table 4 and Figure 2 providers to be appointed in future from CCS Framework RM6088: Construction Works and Associated Services, as well as Frameworks available from Scape and Pagabo.
- **Integrator, EPMS and LLM (Landlord and Lease Management):** This tower includes the Integrator contract with KBR, the EPMS contract with Turner & Townsend and LLM supplied by Cushman and Wakefield Plc.

Annex 2 - Security Policy

1. GENERAL

The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, comply with the Client's security requirements as set out in the Contract which include the requirements set out in this Annex 2 (the "**Security Policy**"). The Security Policy includes, but is not limited to, requirements regarding the confidentiality, integrity and availability of Client Assets, the Client's Systems Environment and the Consultant's Systems Environment.

Terms used in this Annex 2 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 the 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 Client.
"Breach of Security"	means the occurrence of:

	<p>(I) any unauthorised access to or use of Client Data, the Client's Systems Environment (or any part thereof) or the Consultant's Systems Environment (or any part thereof);</p> <p>(II) the loss and/or unauthorised disclosure of any Client Data, the Client's Systems Environment (or any part thereof) or the Consultant's Systems Environment (or any part thereof);</p> <p>(III) any unauthorised event resulting in loss of availability of any Client Data, the Client's Systems Environment (or any part thereof) or the Consultant's Systems Environment (or any part thereof);</p> <p>(IV) any unauthorised changes or modification to any Client Data, the Client's Systems Environment (or any part thereof) or the Consultant's Systems Environment (or any part thereof).</p>
"CHECK"	shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.
"Client Assets"	mean any Client Devices and Client Data.
"Client 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

	<p>electronic, magnetic, optical or tangible media, and which are:-</p> <p>(i) supplied to the Consultant by or on behalf of the Client; or</p> <p>(ii) which the Consultant is required to generate, process, store or transmit pursuant to this contract.</p>
“Client’s Systems Environment”	means all of the Client’s ICT systems which are or may be used for the provision of the <i>services</i> .
“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 <i>services</i> .
“Cyber Essentials”	shall mean the Government-backed, industry-supported scheme managed by the NCSC with higher level of security requirements 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.

<p>“Cyber Security Information Sharing Partnership” or “CiSP”</p>	<p>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.</p>
<p>“Client’s Systems Environment”</p>	<p>means all of the Client’s ICT systems which are or may be used for the provision of the <i>services</i>.</p>
<p>“Good Security Practice”</p>	<p>shall mean:</p> <ul style="list-style-type: none"> 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”	<p>shall mean:</p> <p>a) the protection and preservation of:</p> <p>i) the confidentiality, integrity and availability of any Client Assets, the Client’s Systems Environment (or any part thereof) and the Consultant’s</p>
	<p>Systems Environment (or any part thereof);</p> <p>ii) related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and</p> <p>b) compliance with all Law applicable to the processing, transmission, storage and disposal of Client Assets.</p>
“Information Security Manager”	<p>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.</p>
“Information Security Management System (“ISMS”)	<p>shall mean the set of policies, processes and systems designed, implemented and maintained by the Consultant to manage Information Security Risk as specified by ISO/IEC 27001.</p>
“Information Security Questionnaire”	<p>shall mean the Client’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.</p>

“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	<p>shall mean</p> <p>a) ISO/IEC 27001; b) ISO/IEC 27002/IEC; and c) ISO 22301</p> <p>in each case as most recently published by the International Organization for</p>

	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 Client Assets, the Client’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”	mean the Client’s Security Policies published by the Client from time to time and shall include any successor, replacement or additional Security Policies. The Security Policies are set out in Annex A.
“Security Policies and Standards”	mean the Security Policies and the Security Standards
“Security Standards”	mean the Client’s Security Standards published by the Client 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 Client Assets, the Client’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 Client shall be construed as a notice to be provided by the Consultant to the Client.

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 Contract.
- 3.2 The Consultant shall appoint an Information Security Manager and shall notify the Client 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 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 Client upon request within 10 Working Days from such request.

- 3.3A If the Consultant reasonably considers that it is not reasonably commercially possible for it to comply with paragraphs 3.1 and 3.3 of this Schedule by the start of the *service period*, the Consultant shall:
- a) give written notice to the Client to inform it of the same and complete, in cooperation with the Client, the Information Security Questionnaire within 5 working days of being notified by the Client that the Consultant is the successful Framework Supplier (as defined in the Framework Agreement) in respect of this Contract in accordance with paragraph 6.1 of this Schedule;
 - b) provide to the Client, for its consideration, within 10 working days of being notified by the Client that the Consultant is the successful Framework Supplier (as defined in the Framework Agreement) in respect of this Contract:
 - i. a proposed action plan (including a timetable) indicating how the Consultant will become compliant with paragraphs 3.1 and 3.3 of this Schedule and the dates by which they can reasonably become compliant (assuming the Consultant uses all reasonable endeavours to do so) ("**Proposed ISO27001 Action Plan**"); and

- ii. its proposed Information Security Management System that mitigates the failure to comply with paragraphs 3.1 and 3.3 of this Schedule as far as reasonably commercially possible and which is otherwise compliant with the requirements of this Schedule (“**Proposed ISMS**”), and the Consultant shall make such amendments to the Proposed ISO27001 Action Plan and the Proposed ISMS that the Client shall consider necessary in the interests of complying with this Schedule and managing Information Security Risk. Upon the Client being satisfied with the Proposed ISO27001 Action Plan and Proposed ISMS (following implementation of such amendments it considers necessary) it shall notify the Consultant, upon which they shall become the “**ISO27001 Action Plan**” and “**Interim ISMS**” respectively;
 - c) use all reasonable endeavours to become compliant with paragraphs 3.1 and 3.3 of this Schedule as soon as possible and in any event shall become compliant by no later than the dates set out in the ISO27001 Action Plan; and
 - d) operate and maintain the Proposed ISMS until such time as the Interim ISMS is approved, upon which it will operate and maintain the Interim ISMS, as modified from time to time pursuant to the implementation of the ISO27001 Action Plan. Any breach of this paragraph 3.3A constitutes a substantial failure to comply with the Consultant’s obligations under the Contract.
- 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 Client.
- 3.5 Notwithstanding the provisions of paragraph **Error! Reference source not found.** to paragraph **Error! Reference source not found.**, the Client 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 Client annually on the dates as agreed by the Parties.

4.2 The Consultant shall notify the Client 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.

4.3 If the Consultant reasonably considers that it is not reasonably commercially possible for it to obtain certification to Cyber Essentials by the start of the *service period*, the Consultant shall:

- a) give written notice to the Client to inform it of the same and complete, in cooperation with the Client, the Information Security Questionnaire within 5 working days of being notified by the Client that the Consultant is the successful Framework Supplier (as defined in the Framework Agreement) in respect of this Contract in accordance with paragraph 6.1 of this Schedule;
- b) provide to the Client, for its consideration, within 10 working days of being notified by the Client that the Consultant is the successful Framework Supplier (as defined in the Framework Agreement) in respect of this Contract, a proposed action plan (including a timetable) indicating how certification to Cyber Essentials will be obtained and the date by which it will be obtained (assuming the Consultant uses all reasonable endeavours to do so) ("**Proposed CEP Action Plan**") and the Consultant shall make such amendments to the Proposed CEP Action Plan that the Client shall consider necessary in the interests of complying with this Schedule and managing Information Security Risk. Upon the Client being satisfied with the Proposed CEP Action Plan (following implementation of such amendments it considers necessary) it shall notify the Consultant, upon which it shall become the "**CEP Action Plan**"; and
- c) use all reasonable endeavours to obtain certification to Cyber Essentials soon as possible and in any event shall become compliant by no later than the dates set out in the CEP Action Plan.

Any breach of this paragraph 4.3 constitutes a substantial failure to comply with the Consultant's obligations under the Contract.

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 Client upon request within 10 Working Days of such request. The Client 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 Client 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 Client. The Consultant shall provide the report of the Risk Assessment to the Client, 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 Client 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 Client 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 Client in relation to the Client'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 Client (the "**Information Security Questionnaire**") at least annually or at the request by the Authority. The Contractor shall provide the completed Information Security Questionnaire to the Authority 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 Client'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 Client's System Environment or (iii) at the request of the Client 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 Client. 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 Client in its absolute discretion.

- 6.3 The Client shall be entitled to send an agent appointed by it, or such other person it shall reasonably require to witness the conduct of any Security Test. The Consultant shall provide to the Client 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 Client, the Consultant shall comply with the Security Policy in respect of code development within the Consultant's Systems Environment and the Client'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 Client, 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 Client at its absolute discretion. The Consultant shall provide all such co-operation and assistance in relation to any Security Test conducted by the Client as the Client may reasonably require.
- 6.7 The Client 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 Client upon request within 10 Working Days of such request.
- 7.3 The Consultant shall notify the Client 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 Client may issue instructions to the Consultant to comply with any amended Security Policy as required by the Client, 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 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 – CLIENT SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

<https://www.gov.uk/government/publications/dwp-procurement-security-policies-andstandards>
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-securitycontrols>)
 - 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-andstandards>:

- 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

Annex 4 - The Employer's Expenses Policy

DWP Travel, Accommodation and Expenses Policy (Sept 21 policy)

1. The following principles and guidance are extracted from the Buyers expenses policy and are only intended to be a summary of the key areas and further guidance can be provided by the Buyer upon request from the Supplier, as the policy may change from time to time.
2. When making a claim for any payment the Supplier shall provide the Buyer with reasonably requested documentary evidence of actual expenditure to support the claim.
3. Supplier resources / Contractors can claim expenses for business travel and accommodation where they have to make a journey to another DWP office or to an official meeting not on DWP

premises. Claims for meals / subsistence cannot be made as Supplier resources / contractor day rates are deemed sufficient to cover such costs. Contractors cannot make claims for any meals.

HOTEL ACCOMODATION

Eligibility

1. You can stay overnight in hotel accommodation for a maximum of 30 nights.
2. Hotel accommodation should only be booked for the actual nights you stay in the accommodation and will not be payable during any absence from work or time away from the accommodation unless you are off sick and:
 - are certified medically unfit to travel; or
 - you have a short period of illness of 3 days or less and no appreciable savings would be made if you returned home during your illness.
3. Hotel accommodation can only be used for the night of your last day of duty if you were unable to return to your home by 20:00 hours and subsequently stayed a further night.
- 4.

HOTEL ROOM EXPENDITURE LIMITS

The following regional maximum expenditure limits are in place:

Overnight stay

London	£130
Rest of the country (except London)	£80

RAIL TRAVEL

1. First Class rail travel is not permitted. Economy class only.
2. Restricted/Advance Purchase tickets must be booked for your journey. As well as being the cheapest option this will also ensure that you have a definite train booked and a seat for your journey(s). 'Anytime' tickets should only be purchased where they are the cheapest available ticket.

TAXIS

1. Staff must always consider whether travelling by taxi is a necessity, having considered alternative travel methods, business needs, sustainability issues and increased public scrutiny of expenses and cost.

When Can I use a Taxi?

2. Taxis can only be used where one of the following applies:

- Heavy luggage has to be handled
- A taxi can be shared with colleagues and there is a saving over public transport costs
- There is no suitable method of public transport
- It is necessary due to a long term health problem
- There is a risk to personal safety
- Exceptionally, the saving of official time is important

3. You can only use a taxi where the fare will be under £50 per person per journey. There are no exceptions to this limit and the limit overrides the authorised use reasons above. You cannot claim reimbursement for any tips or gratuities. **AIR TRAVEL (including International Air Travel)**

Key Policy Points

1. Business journeys must only be booked when meeting in person is essential.
2. Air travel can be authorised where, taking into account the full cost and duration of the journey including travel to/from the airport, and potential overnight stays saved, it offers better value for money than alternative methods.
3. The cheapest ticket which meets the travel requirements must be purchased. In most circumstances this will be an Advance or Fixed ticket.
4. Flights within the UK must be Economy class. When you are flying overseas and flight is less than 2.5 hours you must travel in economy class
5. When you are flying overseas and the flight is over 2.5 hours you should agree the most appropriate class of travel taking into account the requirement to spend responsibly and protect the reputation of the department.
6. Business Class tickets and any tickets costing more than £1,000 should not be booked without prior approval from the Permanent Secretary. You must not book 1st class tickets in any circumstances
7. You must not request lounge access unless this is specifically approved as a necessity, after giving consideration to the extra cost and the actual amount of working time intending to spend in the lounge.

REDACTED

Annex 2 - Security Policy

1. GENERAL

The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, comply with the Client's security requirements as set out in the Contract which include the requirements set out in this Annex 2 (the "**Security Policy**"). The Security Policy includes, but is not limited to, requirements regarding the confidentiality, integrity and availability of Client Assets, the Client's Systems Environment and the Consultant's Systems Environment.

Terms used in this Annex 2 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 the 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 Client.
"Breach of Security"	<p>means the occurrence of:</p> <ul style="list-style-type: none"> (I) any unauthorised access to or use of Client Data, the Client'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 Client Data, the Client'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 Client Data, the Client'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 Client Data,

	the Client'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.
"Client Assets"	mean any Client Devices and Client Data.
"Client Data"	<p>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:-</p> <ul style="list-style-type: none"> (i) supplied to the Consultant by or on behalf of the Client; or (ii) which the Consultant is required to generate, process, store or transmit pursuant to this contract.
"Client's Systems Environment"	means all of the Client's ICT systems which are or may be used for the provision of the <i>services</i> .
"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 <i>services</i> .

“Cyber Essentials Plus”	shall mean the Government-backed, industry-supported scheme managed by the NCSC with higher level of security requirements 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.
“Client’s Systems Environment”	means all of the Client’s ICT systems which are or may be used for the provision of the <i>services</i> .

“Good Security Practice”	<p>shall mean:</p> <ul style="list-style-type: none">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; andc) the Government’s security policies, frameworks, standards and guidelines relating to Information Security.
---------------------------------	---

“Information Security”	<p>shall mean:</p> <ul style="list-style-type: none"> a) the protection and preservation of: <ul style="list-style-type: none"> i) the confidentiality, integrity and availability of any Client Assets, the Client’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 Client Assets.
“Information Security Manager”	<p>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.</p>
“Information Security Management System (“ISMS”)	<p>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.</p>
“Information Security Questionnaire”	<p>shall mean the Client’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.</p>
“Information Security Risk”	<p>shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.</p>

<p>“ISO/IEC 27001, ISO/IEC 27002 and ISO 22301</p>	<p>shall mean</p> <ul style="list-style-type: none"> a) ISO/IEC 27001; b) ISO/IEC 27002/IEC; and c) ISO 22301 <p>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.</p>
<p>“NCSC”</p>	<p>shall mean the National Cyber Security Centre or its successor entity (where applicable).</p>
<p>“Penetration Test”</p>	<p>shall mean a simulated attack on any Client Assets, the Client’s Systems Environment (or any part thereof) or the Consultant’s Systems Environment (or any part thereof).</p>
<p>“PCI DSS”</p>	<p>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”).</p>
<p>“Risk Profile”</p>	<p>shall mean a description of any set of risks. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable.</p>
<p>“SSAE 16”</p>	<p>shall mean the Statement on Standards for Attestation Engagements (SSAE) No. 16 as most recently published by the American Institute of Certified Public Accountants or its successor entity (“AICPA”) or the relevant successor or replacement standard which is formally recommended by the AICPA.</p>
<p>“Security Test”</p>	<p>shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.</p>

“Security Policies”	mean the Client’s Security Policies published by the Client from time to time and
	shall include any successor, replacement or additional Security Policies. The Security Policies are set out in Annex A.
“Security Policies and Standards”	mean the Security Policies and the Security Standards
“Security Standards”	mean the Client’s Security Standards published by the Client 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 Client Assets, the Client’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 Client shall be construed as a notice to be provided by the Consultant to the Client.

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, obtain and maintain certification with ISO/IEC 27001 (the “ISO Certificate”) in relation to the *services* during the Contract.

3.2 The ISO Certificate shall be provided by the Consultant to the Client on the dates as agreed by the Parties.

3.3 The Consultant shall appoint:

- a. an Information Security Manager; and
- b. a deputy Information Security Manager who shall have the appropriate experience, authority and expertise to deputise for the Information Security Manager when s/he

is on leave or unavailable for any period of time. The Consultant shall notify the Client 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.

- 3.4 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 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 Client upon request within 10 Working Days from such request.

3.3A

- 3.5 The Consultant shall notify the Client of any failure to obtain an ISO Certificate or a revocation of an ISO 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 an ISO Certificate following such failure or revocation and provide such ISO Certificate within one calendar month of the initial notification of failure or revocation to the Client or on a date agreed by the Parties. For the avoidance of doubt, any failure to obtain and/or maintain an ISO Certificate during the *service period* after the first date on which the Consultant was required to provide the ISO Certificate in accordance with paragraph 3.1 (regardless of whether such failure is capable of remedy) shall constitute a substantial failure to comply with the

Consultant's obligations under the Contract.

- 3.6 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 Client.
- 3.7 Notwithstanding the provisions of paragraph **Error! Reference source not found.** to paragraph **Error! Reference source not found.**, the Client 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 PLUS SCHEME

- 4.1 The Consultant shall, and shall procure that any Sub-Consultant (as applicable) shall, obtain and maintain certification to Cyber Essentials Plus (the “Cyber Essentials Plus Certificate”) in relation to the Services during the *service period*. The Cyber Essentials Plus Certificate shall be provided by the Consultant to the Client annually on the dates as agreed by the Parties.
- 4.2 The Consultant shall notify the Client of any failure to obtain, or the revocation of, a Cyber Essentials Plus 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 Plus Certificate following such failure or revocation. For the avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Plus Certificate during the *service period* after the first date on which the Consultant was required to provide a Cyber Essentials Plus 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.

4.3

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 Client upon request within 10 Working Days of such request. The Client 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 Client 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 Client. The Consultant shall provide the report of the Risk Assessment to the Client, 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 Client 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 Client 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 Client in relation to the Client'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 Client (the "**Information Security Questionnaire**") at least annually or at the request by the Authority. The Contractor shall provide the completed Information Security Questionnaire to the Authority 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 Client'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 Client's System Environment or (iii) at the request of the Client 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 Client. 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 Client in its absolute discretion.
- 6.3 The Client shall be entitled to send an agent appointed by it, or such other person it shall reasonably require to witness the conduct of any Security Test. The Consultant shall provide to the Client 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 Client, the Consultant shall comply with the Security Policy in respect of code development within the Consultant's Systems Environment and the Client'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 Client, 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 Client at its absolute discretion. The Consultant shall provide all such co-operation and assistance in relation to any Security Test conducted by the Client as the Client may reasonably require.
- 6.7 The Client 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 Client upon request within 10 Working Days of such request.
- 7.3 The Consultant shall notify the Client 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 Client may issue instructions to the Consultant to comply with any amended Security Policy as required by the Client, 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 1 occurs which increases the burden on the Consultant pursuant to this 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 shall be a member of the Cyber Security Information Sharing Partnership in accordance with the recommendations by the NCSC during the *service period*. The Consultant shall participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.
- 9.2 The Consultant 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 – CLIENT SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

<https://www.gov.uk/government/publications/dwp-procurement-security-policies-andstandards> 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-securitycontrols>)
- 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-andstandards>:

- 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