

FORM OF AGREEMENT

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

Between

The Department for Work and Pensions (“DWP”)

And

Del Bosque Limited

For the provision of

Critical Security Infrastructure (CSI) Digitalisation Pilot

TABLE OF CONTENTS

1. Form of Agreement
2. Contract Data – Part one (Data provided by the *Client*)
3. Contract Data – Part two (Data provided by the *Consultant*)
4. Additional conditions of contract – Z Clauses
5. Contract Schedule 1 - Statement of Requirements and Scope
6. Contract Schedule 2 - Activity Schedule
7. Contract Schedule 3 - Consultant Proposal
8. Contract Schedule 4 - Government Commercial Function Supplier Code of Conduct
9. Contract Schedule 5 - Client Security Policy
10. Contract Schedule 6 - Key Performance Indicators
11. Contract Schedule 7 - Financial Distress
12. Contract Schedule 8 - GDPR

THIS AGREEMENT is made the

PARTIES:

1. **THE SECRETARY OF STATE FOR WORK AND PENSIONS** acting as part of the Crown (the "**Client**"); and
2. **DEL BOSQUE LIMITED** which is a company incorporated in and in accordance with the laws of England and Wales (Company No. 13255942) whose registered office address is at Lifford Hall, Lifford Lane, Kings Norton, Birmingham B30 3JN(the "**Consultant**").

BACKGROUND

- (A) The *Consultant* has agreed to Provide the Services in accordance with this agreement.

IT IS AGREED AS FOLLOWS:

1. The *Client* will pay the *Consultant* the amount due and carry out his duties in accordance with the *conditions of contract* identified in the Contract Data and the Contract Schedules.
2. The *Consultant* will Provide the Service in accordance with the *conditions of contract* identified in the Contract Data and the Contract Schedules.
3. This contract incorporates the conditions of contract in the form of the NEC4 Professional Services Contract June 2017 Edition incorporating amendments January 2019 and October 2020 and incorporating the following Options:
 - Main Option A;
 - Dispute Resolution Option W2;
 - Secondary Options X2, X10, X11, X18, and X20
 - Option Y(UK)2

Together with the following Contract Schedules:

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

7. Contract Schedule 7 - Financial Distress

8. Contract Schedule 8 - GDPR

which together with the *additional conditions of contract* specified in Option Z, and the amendments specified in Option Z, form this contract together with the documents referred to in it. References in the NEC4 Professional Services Contract June 2017 Edition incorporating amendments January 2019 and October 2020 to "the contract" are references to this contract.

4. This contract is the entire agreement between the parties in relation to the service and supersedes and extinguishes all prior arrangements, understandings, agreements, statements, representations or warranties (whether written or oral) relating thereto.
5. Neither party has been given, nor entered into this contract in reliance on any arrangements, understandings, agreements, statements, representations or warranties other than those expressly set out in this agreement.
6. Nothing in clauses 4 or 5 shall exclude liability in respect of misrepresentations made fraudulently.

Executed under hand

Signed by **REDACTED** for and on behalf of **DEL BOSQUE LIMITED**

.....

[]

Director

The Client

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

.....

[]

Authorised Signatory

Professional Services Contract

Contract Data

Part one – Data provided by the *Client*

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

Main Option A

Option for resolving and avoiding disputes W2

Secondary Options X2, X10, X11, X18, X20, Y(UK)2 and Z clauses.

- The *service* is as set out in The Statement of Requirements and Scope (Contract Schedule 1) appended to this agreement.
- The *Client* is Department for Work and Pensions of Caxton House, Tothill Street, London, SW1H 9NA.

Address for communications:

Caxton House, Tothill St, London, SW1H 9NA

Address for electronic communications: **REDACTED**

The *Service Manager* is **REDACTED**

Address for communications:

Department for Work & Pensions,
People, Capability and Place – Estates, 2nd Floor, Hartshead Square,
Sheffield

Address for electronic communications: **REDACTED**

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

The *language of the contract* is English.

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

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

The *period for reply* is two weeks.

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

The following matters will be included in the Early Warning Register
N/A

Early warning meetings will be held as and when early warnings are raised by either the Consultant or the Client.

2 The Consultant's main responsibilities

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

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

<i>condition</i> to be met	<i>key date</i>
Completion of progress reports and attendance at meeting(s)	within timescales communicated in writing (which may include email) by the Client to the Consultant as and when required
Notice of planned absence of Consultant Key Personnel e.g. annual leave	at least 10 Working Days prior to the first day of the planned absence

If Option A is used

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

3 Time

The starting date is 5th December 2022

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

- access to *access date*
DWP premises as necessary.

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

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

The *completion date* for the whole of the service is 3rd March 2023.

4 Quality Management

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

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

5 Payment

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

The *assessment interval* is monthly

If the *Client* states any expenses

The *expenses* stated by the *Client* are

Item	Amount
N/A	

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

6 Compensation events

If there are additional compensation events

These are additional compensation events

N/A

8 Liability and insurance

If there are additional *Client* liabilities These are additional *Client* liabilities
1 N/A

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

event	cover	Period
The <i>Consultant's</i> failure to use the skill and care normally used by professionals providing services similar to the <i>service</i>	REDACTED in respect of each event, without limit to the number of events except for claims arising out of pollution or contamination, where the minimum amount of cover applies in the aggregate in any one period of insurance and except for claims arising out of asbestos where a lower level may apply in the aggregate	from the <i>starting date</i> until 6 years following completion of the whole of the <i>service</i> or earlier termination

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

Resolving and avoiding disputes The tribunal is arbitration

If the *tribunal* is arbitration The *arbitration procedure* is the London Court of International Arbitration Rules;
The place where arbitration is to be held is London
The person or organisation who will choose the arbitrator if the parties cannot agree a choice or if the *arbitration procedure* does not state who selects and arbitrator is: Royal Institution of Chartered Surveyors.

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

Address for communications:

Department for Work & Pensions, Quarry House, Leeds, LS2 7UA

Address for electronic communications: **REDACTED**

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

Address for communications:

Department for Work & Pensions,
People, Capability and Place – Estates, 2nd Floor, Hartshead Square,
Sheffield

Address for electronic communications: **REDACTED**

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

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

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

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

Option X1 **Option X1 is not used**

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

Option X3 Option X3 is not used

Option X5 Option X5 is not used

Option X6 Option X6 is not used

Option X7 Option X7 is not used

Option X8 Option X8 is not used

Option X10 If Option X10 is used
Information
modelling

If no *information execution plan* is identified in part two of the Contract Data The period after the Contract Date within which the *Consultant* is to submit a first Information Execution Plan for acceptance is two weeks.

Option X12 Option X12 is not used

Option X13 Option X13 is not used

Option X18 If Option X18 is used
Limitation of
liability

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

Option X20 Key performance indicators

The *incentive schedule* for Key Performance Indicators is in Contract Schedule 6.

Unless otherwise communicated by the Client to the Consultant, a report of performance against each Key Performance Indicator is provided by the Consultant to the Client at monthly intervals.

- The Parties shall meet within 5 Working Days following each KPI performance report being provided at a Performance Review Meeting. Without prejudice to the Improvement Plan Process set out below, actions and associated timescales will be agreed to share best practice and/or agree how improvements to performance will be implemented.
- The performance of the Consultant in the preceding month is classified as 'Good' if KPIs 1 to 4 are marked as Green.
- The performance of the Consultant in the preceding month is classified as 'Poor' if two or more of the KPIs are marked as Red.
- The performance of the Consultant in the preceding month is classified as 'Requiring Improvement' if the Key Performance Indicators are neither classified as 'Good' or 'Poor.'
- Where X20 is used, the amount due under clause 50 is adjusted to account for the application of the *incentive schedule*.
- The *Client* reserves the right to disapply the *incentive schedule* where the *Client* considers that mitigating circumstances apply.

Improvement Plan Process

- An **Improvement Plan** is the plan to address the impact of and prevent the reoccurrence of performance by the *Consultant* which is 'Poor' or 'Requiring Improvement'.
- Where the performance of the *Consultant* is 'Poor' or 'Requiring Improvement' in the previous month, the *Client* may serve notice (an **Improvement Notice**) on the *Consultant* setting out sufficient detail to make it clear what the *Consultant* has to rectify.
- Where an Improvement Notice is served the *Consultant* submits to the *Client* a draft Improvement Plan and the *Client* reviews it as soon as possible and in any event within 10 Working Days (as defined in Contract Schedule 5) (or such other period as the Parties agree) of the monthly performance meeting or, if later, the date of service of the Improvement Notice. The *Consultant* submits a draft Improvement Plan even if it disputes the performance rating in the previous month.

- The draft Improvement Plan sets out:
 1. full details of the performance rating in the previous month and which KPIs were rated as Red or Amber to achieve this rating; and
 2. the steps the *Consultant* proposes to take to rectify and improve the performance of these KPIs and to prevent any issues from recurring, including timescales for such steps.
- The *Consultant* provides the *Client* with such additional information or documentation as the *Client* reasonably requires.
- The *Client* notifies the *Consultant* that:
 1. it agrees the draft Improvement Plan; or
 2. it rejects the draft Improvement Plan because it is inadequate, for example because it is not detailed enough to evaluate, will take too long to complete, will not prevent reoccurrence of the Red or Amber markings it was drafted to improve or is otherwise unacceptable to the *Client*. Where the *Client* does so it shall set out its reasons for doing so.
- Where the *Client* accepts the Improvement Plan the *Consultant* immediately implements the actions in the Improvement Plan.
- Where the *Client* rejects the Improvement Plan the *Consultant* resubmits its draft Improvement Plan taking into account the *Client's* comments within 5 Working Days of notice that the *Client* rejects the preceding Improvement Plan.
- Without prejudice to any other right or remedy of the *Client*, the *Client* may terminate this contract by written notice to the *Consultant* if performance of the *Consultant* is classified as 'Poor' in three or more consecutive months and the *Consultant* fails in respect of any of such incidences of 'Poor' performance:
 1. to submit a draft Improvement Plan to the *Client*;
 2. to submit a draft Improvement Plan which the *Client* acting reasonably does not approve;
 3. to implement an Improvement Plan agreed by the Parties by the date of rectification stipulated in the Improvement Plan; or
 4. following implementation of a previous Improvement Plan, where one or more of the same KPIs has received a Red marking in consecutive months for the same (or substantially the same) root cause.

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

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

Option Z The *additional conditions of contract* are: Z2, Z5, Z6, Z7, Z8, Z9, Z10, Z13, Z14, Z16, Z22, Z44, Z48, Z49, Z50, Z51, Z52, Z53 and Z54

Contract Data relating to Z clauses The additional conditions of contract are as set out below.

Option Z2 **Identified and defined terms** Insert new clause 11.3 additional defined terms.

11.3 (1) Auditor is:

- the *Client's* internal and external auditors;
- the *Client's* statutory or regulatory auditors;
- the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office;
- HM Treasury or the Cabinet Office;
- any party formally appointed by the *Client* to carry out audit or similar review functions; and
- successors or assigns of any of the above;

11.3 (2) Change of Control is a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;

11.3 (3) Client Confidential Information is all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and contractors of the *Client* and/or any of the *Client's* other suppliers, including all IPRs and all financial or pricing information, together with all information derived from any of the above, and any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered to be confidential.

11.3 (4) Client Data is the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these)

which are embodied in any electronic, magnetic, optical or tangible media, and

- which are supplied to the *Consultant* by or on behalf of the *Client*,
- which the *Consultant* is required to generate, process, store or transmit pursuant to this contract or
- which are any Personal Data for which the *Client* is the Data Controller to the extent that such Personal Data is held or processed by the *Consultant*.

11 (5) *Client's Premises* are premises owned, occupied or leased by the *Client* and the site of any works to which the *service* relates.

11.3 (6) *Commercially Sensitive Information* is the information agreed between the Parties (if any) comprising the information of a commercially sensitive nature relating to the *Consultant*, the charges for the *service*, its IPR or its business or which the *Consultant* has indicated to the *Client* that, if disclosed by the *Client*, would cause the *Consultant* significant commercial disadvantage or material financial loss.

11.3 (7) *Confidential Information* is the *Client's Confidential Information* and/or the *Consultant's Confidential Information*.

11.3 (8) *Contracting Body* is any *Contracting Body* as defined in Regulation 5(2) of the Public Contracts (Works, Service and Supply) (Amendment) Regulations 2000 other than the *Client*.

11.3 (9) *Consultant's Confidential Information* is any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and consultants of the *Consultant*, including IPRs, together with all information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential, including the *Commercially Sensitive Information*.

11.3 (10) *Crown Body* is any department, office or agency of the Crown.

11.3 (11) *DASVOIT* is the Disclosure of Tax Avoidance Schemes: VAT and other indirect taxes contained in the Finance (No.2) Act 2017.

11.3 (12) DOTAS is the Disclosure of Tax avoidance Schemes rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.

11.3 (13) Environmental Information Regulations is the Environmental Information Regulations 2004 and any guidance and/or codes of practice issued by the Information Commissioner in relation to such regulations.

11.3 (14) FOIA is the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner in relation to such legislation.

11.3 (15) General Anti-Abuse Rule is

- the legislation in Part 5 of the Finance Act 2013 (as amended) and
- any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements and to avoid national insurance contributions.

11.3 (16) Halifax Abuse Principle is the principle explained in the CJEU Case C-255/02 Halifax and others.

11.3 (17) Intellectual Property Rights or "IPRs" is

- copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information,
- applications for registration, and the right to apply for registration, for any of the rights listed in the first bullet point that are capable of being registered in any country or jurisdiction,

- all other rights having equivalent or similar effect in any country or jurisdiction and
- all or any goodwill relating or attached thereto.

11.3 (18) Law is any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the *Consultant* is bound to comply under the *law of the contract*.

11.3 (19) An Occasion of Tax Non-Compliance is

- where any tax return of the *Consultant* submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of
- a Relevant Tax Authority successfully challenging the *Consultant* under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle or
- the failure of an avoidance scheme which the *Consultant* was involved in, and which was, or should have been, notified to a Relevant Tax Authority under DASVOIT, DOTAS or VADR or any equivalent or similar regime and

where any tax return of the *Consultant* submitted to a Relevant Tax Authority on or after 1 October 2012 gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Contract Date or to a civil penalty for fraud or evasion.

11.3 (20) Prohibited Act is

- to directly or indirectly offer, promise or give any person working for or engaged by the *Client* or other Contracting Body or any other public body a financial or other advantage to
- induce that person to perform improperly a relevant function or activity or
- reward that person for improper performance of a relevant

function or activity,

- to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this contract,
- committing any offence
 - under the Bribery Act 2010 (or any legislation repealed or revoked by such Act),
 - under legislation or common law concerning fraudulent acts or
 - defrauding, attempting to defraud or conspiring to defraud the *Client* or
- any activity, practice or conduct which would constitute one of the offences listed above if such activity, practice or conduct had been carried out in the UK.

11.3 (21) Request for Information is a request for information or an apparent request under the Code of Practice on Access to government Information, FOIA or the Environmental Information Regulations.

11.3 (22) Relevant Requirements are all applicable Laws relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010.

11.3 (23) Relevant Tax Authority is HM Revenue & Customs, or, if applicable, a tax authority in the jurisdiction in which the *Consultant* is established.

11.3 (24) Security Policy means the *Client's* security policy attached as Contract Schedule 5 as may be updated from time to time.

11.3 (25) VADR is the VAT disclosure regime under Schedule 11A of the Value Added Tax Act 1994 (VATA 1994) (as amended by Schedule 1 of the Finance (No. 2) Act 2005).

Option Z5 Prevention of fraud and bribery

Insert new clauses:

17.4.1 The *Consultant* represents and warrants that neither it, nor to the best of its knowledge any of its people, have at any time prior to the Contract Date

- committed a Prohibited Act or been formally notified that it is subject to an investigation or prosecution which relates to an alleged Prohibited Act or
- been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act.

17.4.2 During the carrying out of the service the *Consultant* does not

- commit a Prohibited Act and
- do or suffer anything to be done which would cause the *Client* or any of the *Client's* employees, consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements.

17.4.3 In Providing the Service the *Consultant*

- establishes, maintains and enforces, and requires that its Subcontractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act,
- keeps appropriate records of its compliance with this contract and make such records available to the *Client* on request and
- provides and maintains and where appropriate enforces an anti-bribery policy (which shall be disclosed to the *Client* on request) to prevent it and any *Consultant's* people or any person acting on the *Consultant's* behalf from committing a Prohibited Act.

17.4.4 The *Consultant* immediately notifies the *Client* in writing if it becomes aware of any breach of clause 17.4.1, or has reason to believe that it has or any of its people or Subcontractors have

- been subject to an investigation or prosecution which relates to an alleged Prohibited Act,
- been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act or
- received a request or demand for any undue financial or other advantage of any kind in connection with the performance of this contract or otherwise suspects that any person or party directly or indirectly connected with this contract has committed or attempted to commit a Prohibited Act.

17.4.5 If the *Consultant* makes a notification to the *Client* pursuant to clause 17.4.4, the *Consultant* responds promptly to the *Client's* enquiries, co-operates with any investigation, and allows the *Client* to audit any books, records and/or any other relevant documentation in accordance with this contract.

17.4.6 If the *Consultant* breaches Clause 17.4.3, the *Client* may by notice require the *Consultant* to remove from carrying out the *service* any person whose acts or omissions have caused the *Consultant's* breach.

Option Z6 Equality and diversity

27.1 The *Consultant* performs its obligations under this contract in accordance with

- all applicable equality Law (whether in relation to race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise); and
- any other requirements and instructions which the *Client* reasonably imposes in connection with any equality obligations imposed on the *Client* at any time under applicable equality Law;

27.2 The *Consultant* takes all necessary steps, and informs the *Client* of the steps taken, to prevent unlawful discrimination designated as such by any court or tribunal, or the Equality and Human Rights Commission or (any successor organisation).

Option Z7 Legislation and Official Secrets

20.6 The *Consultant* complies with Law in the carrying out of the service.

20.7 The Official Secrets Acts 1911 to 1989, section 182 of the Finance Act 1989 and, where appropriate, the provisions of section 11 of the Atomic Energy Act 1946 apply to this contract.

20.8 The *Consultant* notifies its employees and its Subcontractors of their duties under these Acts.

Option Z8 Conflict of interest

28.1. The *Consultant* takes appropriate steps to ensure that neither the *Consultant* nor any of its personnel are placed in a position where (in the reasonable opinion of the *Client*) there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the *Consultant* or its personnel and the duties owed to the *Client* under this contract.

28.2. The *Consultant* promptly notifies and provides full particulars to the *Client* if such conflict referred to in clause 28.1 arises or may reasonably be foreseen as arising.

28.3. The *Client* may terminate the *Consultant's* obligation to Provide the Service immediately under reason R11 and/or to take such other steps the *Client* deems necessary where, in the reasonable opinion of the *Client*, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the *Consultant* and the duties owed to the *Client* under this contract.

Option Z9 Publicity and Branding

29.1 The *Consultant* does not

- make any press announcements or publicise this contract in any way
- use the *Client's* name or brand in any promotion or marketing

or announcement of the contract

without approval of the *Client*.

29.2. The *Client* is entitled to publicise the contract in accordance with any legal obligation upon the *Client*, including any examination of the contract by the National Audit Office pursuant to the National Audit Act 1983 or otherwise.

Option Z10 Freedom of information

26.2 The *Consultant* acknowledges that unless the *Service Manager* has notified the *Consultant* that the *Client* is exempt from the provisions of the FOIA, the *Client* is subject to the requirements of the Code of Practice on Government Information, the FOIA and the Environmental Information Regulations. The *Consultant* cooperates with and assists the *Client* so as to enable the *Client* to comply with its information disclosure obligations.

26.3 The *Consultant*

- transfers to the *Service Manager* all Requests for Information that it receives as soon as practicable and in any event within two working days of receiving a Request for Information,
- provides the *Service Manager* with a copy of all information in its possession, or power in the form that the *Service Manager* requires within five working days (or such other period as the *Service Manager* may specify) of the *Service Manager's* request,
- provides all necessary assistance as reasonably requested by the *Service Manager* to enable the *Client* to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations and
- procures that its Subcontractors do likewise.

26.4 The *Client* is responsible for determining in its absolute discretion whether any information is exempt from disclosure in accordance with the provisions of the Code of Practice on Government Information, FOIA or the Environmental Information Regulations.

26.5 The *Consultant* does not respond directly to a Request for Information unless authorised to do so by the *Service Manager*.

26.6 The *Consultant* acknowledges that the *Client* may, acting in accordance with Cabinet Office Freedom of Information Code of Practice, be obliged to disclose information without consulting or obtaining consent from the *Consultant* or despite the *Consultant* having expressed negative views when consulted.

26.7 The *Consultant* ensures that all information is retained for disclosure throughout the *period for retention* and permits the *Service Manager* to inspect such records as and when reasonably requested from time to time.

Option Z13 Confidentiality and Information Sharing

26.8 Except to the extent set out in this clause or where disclosure is expressly permitted elsewhere in this contract, each Party shall

- treat the other Party's Confidential Information as confidential and safeguard it accordingly,
- not disclose the other Party's Confidential Information to any other person without prior written consent,
- immediately notify the other Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information and
- notify the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

26.9 The clause above shall not apply to the extent that

- such disclosure is a requirement of the Law placed upon the party making the disclosure, including any requirements for disclosure under the FOIA or the Environmental Information Regulations pursuant to clause Z10 (Freedom of Information),
- such information was in the possession of the party making the disclosure without obligation of confidentiality prior to its

disclosure by the information owner,

- such information was obtained from a third party without obligation of confidentiality,
- such information was already in the public domain at the time of disclosure otherwise than by a breach of this contract or
- it is independently developed without access to the other party's Confidential Information.

26.10 The *Consultant* may only disclose the Client Confidential Information to the people who are directly involved in Providing the Service and who need to know the information, and shall ensure that such people are aware of and shall comply with these obligations as to confidentiality. The *Consultant* shall not, and shall procure that the *Consultant's* people do not, use any of the Client Confidential Information received otherwise than for the purposes of this contract.

26.11 The *Consultant* may only disclose the Client Confidential Information to *Consultant's* people who need to know the information, and shall ensure that such people are aware of, acknowledge the importance of, and comply with these obligations as to confidentiality. In the event that any default, act or omission of any *Consultant's* people causes or contributes (or could cause or contribute) to the *Consultant* breaching its obligations as to confidentiality under or in connection with this contract, the *Consultant* shall take such action as may be appropriate in the circumstances, including the use of disciplinary procedures in serious cases. To the fullest extent permitted by its own obligations of confidentiality to any *Consultant's* people, the *Consultant* shall provide such evidence to the *Client* as the *Client* may reasonably require (though not so as to risk compromising or prejudicing the case) to demonstrate that the *Consultant* is taking appropriate steps to comply with this clause, including copies of any written communications to and/or from *Consultant's* people, and any minutes of meetings and any other records which provide an audit trail of any discussions or exchanges with *Consultant's* people in connection with obligations as to confidentiality.

26.12 At the written request of the *Client*, the *Consultant* shall procure that those members of the *Consultant's* people identified in the *Client's* request signs a confidentiality undertaking prior to commencing any work in accordance with this contract.

26.13 Nothing in this contract shall prevent the *Client* from disclosing the Consultant's Confidential Information

- to any Crown Body or any other Contracting Bodies. All Crown Bodies or Contracting Bodies receiving such Confidential Information shall be entitled to further disclose the Consultant's Confidential Information to other Crown Bodies or other Contracting Bodies on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Crown Body or any Contracting Body,
- to a professional adviser, contractor, consultant, supplier or other person engaged by the *Client* or any Crown Body (including any benchmarking organisation) for any purpose connected with this contract, or any person conducting an Office of Government Commerce Gateway Review,
- for the purpose of the examination and certification of the *Client's* accounts,
- for any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the *Client* has used its resources,
- for the purpose of the exercise of its rights under this contract or
- to a proposed successor body of the *Client* in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under this contract,

and for the purposes of the foregoing, disclosure of the Consultant's Confidential Information shall be on a confidential basis and subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the *Client* under this clause 26.13.

26.14 The *Client* shall use all reasonable endeavours to ensure that any government department, Contracting Body, people, third party or subcontractor to whom the Consultant's Confidential Information is disclosed pursuant to the above clause is made aware of the *Client's* obligations of confidentiality.

26.15 Nothing in this clause shall prevent either party from using any techniques, ideas or know-how gained during the performance of the contract in the course of its normal business to the extent that this use

does not result in a disclosure of the other party's Confidential Information or an infringement of IPR.

26.16 The *Client* may disclose the Consultant's Confidential Information

- to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement,
- to the extent that the *Client* (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions.

Option Z14 Security Requirements

The *Consultant* complies with, and procures the compliance of the *Consultant's* people, with the Security Policy and the Security Management Plan produced by the *Consultant* and the *Consultant* shall ensure that the Security Management Plan fully complies with the Security Policy and Contract Schedule 5.

Option Z16 Tax Compliance

- 26.17 The *Consultant* represents and warrants that at the Contract Date, it has notified the *Client* in writing of any Occasions of Tax Non-Compliance or any litigation that it is involved in that is in connection with any Occasions of Tax Non-Compliance.
- 26.18 If, at any point prior to the *defects date*, an Occasion of Tax Non-Compliance occurs, the *Consultant* shall
 - notify the *Client* in writing of such fact within 5 days of its occurrence and
 - promptly provide to the *Client*
 - details of the steps which the *Consultant* is taking to address the Occasions of Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant and
 - such other information in relation to the Occasion of Tax Non-Compliance as

the *Client* may reasonably require.

Option Z22 Fair payment applies

56.1 The *Consultant* assesses the amount due to a Subcontractor without taking into account the amount certified by the *Service Manager*.

56.2 The *Consultant* includes in the contract with each Subcontractor

- a period for payment of the amount due to the Subcontractor not greater than 5 days after the final date for payment in this contract. The amount due includes, but is not limited to, payment for work which the Subcontractor has completed from the previous assessment date up to the current assessment date in this contract,
- a provision requiring the Subcontractor to include in each subsubcontract the same requirement (including this requirement to flow down, except that the period for payment is to be not greater than 9 days after the final date for payment in this contract and
- a provision requiring the Subcontractor to assess the amount due to a subsubcontractor without taking into account the amount paid by the *Consultant*.

Option Z44 Intellectual Property Rights

“Document” means all designs, drawings, specifications, software, electronic data, photographs, plans, surveys, reports, and all other documents and/or information prepared by or on behalf of the *Consultant* in relation to this contract.

70.1 The Intellectual Property Rights in all Documents prepared by or on behalf of the *Consultant* in relation to this contract and the work executed from them remains the property of the *Consultant*. The *Consultant* hereby grants to the *Client* an irrevocable, royalty free, non-exclusive licence to use and reproduce the Documents for any and all purposes connected with the construction, use, alterations or demolition of the *service*. Such licence entitles the *Client* to grant sub-licences to third parties in the same terms as this

licence provided always that the *Consultant* shall not be liable to any licensee for any use of the Documents or the Intellectual Property Rights in the Documents for purposes other than those for which the same were originally prepared by or on behalf of the *Consultant*.

70.2 The *Client* may assign novate or otherwise transfer its rights and obligations under the licence granted pursuant to clause 70.1 to a Crown Body or to anybody (including any private sector body) which performs or carries on any functions and/or activities that previously had been performed and/or carried on by the *Client*.

70.3 In the event that the *Consultant* does not own the copyright or any Intellectual Property Rights in any Document the *Consultant* uses all reasonable endeavours to procure the right to grant such rights to the *Client* to use any such copyright or Intellectual Property Rights from any third party owner of the copyright or Intellectual Property Rights. In the event that the *Consultant* is unable to procure the right to grant to the *Client* in accordance with the foregoing the *Consultant* procures that the third party grants a direct licence to the *Client* on industry acceptable terms.

70.4 The *Consultant* waives any moral right to be identified as author of the Documents in accordance with section 77, Copyright Designs and Patents Acts 1988 and any right not to have the Documents subjected to derogatory treatment in accordance with section 8 of that Act as against the *Client* or any licensee or assignee of the *Client*.

70.5 In the event that any act unauthorised by the *Client* infringes a moral right of the *Consultant* in relation to the Documents the *Consultant* undertakes, if the *Client* so requests and at the *Client's* expense, to institute proceedings for infringement of the moral rights.

70.6 The *Consultant* warrants to the *Client* that it has not granted and shall not (unless authorised by the *Client*) grant any rights to any third party to use or otherwise exploit the Documents.

70.7 The *Consultant* supplies copies of the Documents to the *Service Manager* and to the *Client's* other contractors and consultants for no additional fee to the extent necessary to enable them to discharge their respective functions in relation to this contract or related service.

70.8 After the termination or conclusion of the *Consultant's* employment hereunder, the *Consultant* supplies the *Service Manager* with copies and/or computer discs of such of the Documents as the *Service Manager* may from time to time request

and the *Client* pays the *Consultant's* reasonable costs for producing such copies or discs.

70.9 In carrying out the *service* the *Consultant* does not infringe any Intellectual Property Rights of any third party. The *Consultant* indemnifies the *Client* against claims, proceedings, compensation and costs arising from an infringement or alleged infringement of the Intellectual Property Rights of any third party.

Option Z48 Apprenticeships applies

23.5 The *Consultant* takes all reasonable steps to employ apprentices, and reports to the *Client* the numbers of apprentices employed and the wider skills training provided, during the delivery of the *service*.

The *Consultant* takes all reasonable steps to ensure that no less than a percentage of its people (agreed between the Parties) are on formal apprenticeship programmes or that a similar proportion of hours worked in Providing the Service, (which may include support staff and Subcontractors) are provided by people on formal apprenticeship programmes.

The *Consultant* makes available to its people and Subcontractors working on the contract, information about the Government's Apprenticeship programme and wider skills opportunities.

The *Consultant* provides any further skills training opportunities that are appropriate for its people engaged in Providing the Service.

The *Consultant* provides a report detailing the following measures in its regular contract management monthly reporting cycle and is prepared to discuss apprenticeships at its regular meetings with the *Service Manager*

- the number of people during the reporting period employed on the contract, including support staff and Subcontractors,
- the number of apprentices and number of new starts on apprenticeships directly initiated through this contract,
- the percentage of all people taking part in an apprenticeship programme,
- if applicable, an explanation from the *Consultant* as to why it

is not managing to meet the specified percentage target,

- actions being taken to improve the take up of apprenticeships and
- other training/skills development being undertaken by people in relation to this contract, including:
 - (a) work experience placements for 14 to 16 year olds,
 - (b) work experience /work trial placements for other ages,
 - (c) student sandwich/gap year placements,
 - (d) graduate placements,
 - (e) vocational training,
 - (f) basic skills training and
 - (g) on site training provision/ facilities.

Option Z49 Change of Control

19.1 The *Consultant* notifies the *Client* and the *Service Manager* immediately in writing and as soon as the *Consultant* is aware (or ought reasonably to be aware) that it is anticipating, undergoing, undergoes or has undergone a Change of Control and provided such notification does not contravene any Law. The *Consultant* ensures that any notification sets out full details of the Change of Control including the circumstances suggesting and/or explaining the Change of Control.

91.9 The *Client* may terminate the *Consultant's* obligation to Provide the Service (which shall take effect as termination under reason R11) within six months from

- being notified in writing that a Change of Control is anticipated or is in contemplation or has occurred; or
- where no notification has been made, the date that the *Client* becomes aware that a Change of Control is anticipated or is in contemplation or has occurred, but shall not be permitted to terminate where an approval was granted prior to the Change of

Control.

Option Z50 Financial Standing

91.10 The *Client* may terminate the *Consultant's* obligation to Provide the Service (which shall take effect as termination under reason R11) where in the reasonable opinion of the *Client* there is a material detrimental change in the financial standing and/or the credit rating of the *Consultant* which:

- adversely impacts on the *Consultant's* ability to perform its obligations under this contract; or
- could reasonably be expected to have an adverse impact on the *Consultant's* ability to perform its obligations under this contract.

Option Z51 Financial Distress

The *Consultant* complies with the provisions of Contract Schedule 7 (Financial Distress) in relation to the assessment of the financial standing of the *Consultant* and the consequences of a change to that financial standing.

Option Z52 Records, audit access and open book data

26A.1 The *Consultant* keeps and maintains for the *period for retention* full and accurate records and accounts of the operation of this contract including the service provided under it, any subcontracts and the amounts paid by the *Client*.

26A.2 The *Consultant*

- keeps the records and accounts referred to in clause 26A.1 in accordance with Law
- affords any Auditor access to the records and accounts referred to in clause 26A.1 at the *Consultant's* premises and/or provides records and accounts (including copies of the *Consultant's* published accounts) or copies of the same, as may be required by any Auditor from time to time during the *Consultant* Providing the Service and the liability period under the contract in order that the Auditor may carry out an inspection to assess compliance by the *Consultant* and/or its

Subcontractors of any of the *Consultant's* obligations under this contract including in order to:

- verify the accuracy of any amounts payable by the *Client* under this contract (and proposed or actual variations to them in accordance with this contract)
- verify the costs of the *Consultant* (including the costs of all Subcontractors and any third party suppliers) in connection with Providing the Service
- identify or investigate an actual or suspected Prohibited Act, impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the *Client* has no obligation to inform the *Consultant* of the purpose or objective of its investigations
- obtain such information as is necessary to fulfil the *Client's* obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General
- enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the *Client* has used its resources
- subject to the *Consultant's* rights in respect of Consultant's Confidential Information, the *Consultant* provides the Auditor on demand with all reasonable co-operation and assistance in respect of
 - all reasonable information requested by the *Client* within the scope of the audit
 - reasonable access to sites controlled by the *Consultant* and to any *Consultant's* equipment used to Provide the Service
 - access to the *Consultant's* personnel.

26A.3 The Parties bear their own respective costs and expenses incurred in respect of compliance with their obligations under this clause 26A, unless the audit reveals a default by the *Consultant* in

which case the *Consultant* reimburses the *Client* for the *Client's* reasonable costs incurred in relation to the audit.

26A.4 This clause does not constitute a requirement or agreement for the purposes of section 6(3)(d) of the National Audit Act 1983 for the examination, certification or inspection of the accounts of the *Consultant* and the carrying out of an examination under Section 6(3)(d) of the National Audit Act 1983 in relation to the *Consultant* is not a function exercisable under this contract.

Option Z53 Data Protection

The *Client* and the *Consultant* shall comply with the provisions of Contract Schedule 8.

Option Z54 Third party conflicts of interest

Insert new clauses:

28.4 For the purposes of clauses 28.4 to 28.7 the following terms have the following meanings:

- “Affiliate” means an entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time
- “contracting authority” has the meaning given to it in regulation 2 of the Public Contracts Regulations 2015
- “Control” has the meaning given to it in section 1124 of the Corporation Tax Act 2010
- “procurement” has the meaning given to it in regulation 2 of the Public Contracts Regulations 2015
- “Representative” refers to a person's officers, directors, employees, advisers and agents and, where the context admits, providers or potential providers of finance to the *Consultant* or any Affiliate in connection with a procurement and the representatives of such providers or potential providers of finance

28.5 The *Consultant* acknowledges and agrees that a conflict of interest may arise in situations where the *Consultant* or an affiliate

(being an entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time) intends to participate in a procurement (whether for the *Client* or any other contracting authority) and, because of the *Consultant's* relationship with the *Client* under this contract, the *Consultant*, its affiliates and/or representatives (as defined below) have or have had access to information which could provide the *Consultant* and/or its affiliates with an advantage and render unfair an otherwise genuine and open competitive procurement process.

28.6 The *Consultant* agrees that it shall notify any relevant Contracting Authority immediately of all perceived, potential and/or actual conflicts of interest that arise in the situation described in clause 28.5 above and shall take all appropriate steps to ensure that the *Consultant* and its Affiliates and/or Representatives:

- are not in a position where, in the reasonable opinion of the relevant Contracting Authority, there is or may be an actual conflict, or a potential conflict; and
- are not provided with an advantage that might render unfair an otherwise genuine and open competitive procurement process by virtue of any information accessed under or in connection with this contract.

28.7 The obligations of the *Consultant* under this clause 28 shall continue for the duration of this contract and for 1 year following its termination or expiry.

**Other Additional
conditions of
contract** n/a

Part two – Data provided by the *Consultant*

**1 Statements given
in all contracts** The *Consultant* is DEL BOSQUE LIMITED

- *Address for communications*

*Office 6 Wassell Grove Business Centre, Wassell Grove Lane,
Stourbridge DY9 9JH*

Address for electronic communications **REDACTED**

The *fee percentage* is n/a

- The *key persons* are as provided in Contract Schedule 3 - Consultant Proposal.

The following matters will be included in the Early Warning Register

- n/a

2 The *Consultant's* main responsibilities

If the *Consultant* is to provide the Scope n/a

3 Time

If a programme is to be identified in the Contract Data The programme identified in the Contract Data is as per the supplier's proposal for the activities contained within the Activity Schedule.

If the *Consultant* is to decide the completion date for the whole of the service The *completion date* for the whole of the service is 3rd March 2023

5 Payment

If the *Consultant* states any expenses The *expenses* stated by the *Consultant* are

• item	• amount
• N/A	

If Option A or C is used The *activity schedule* is defined in Contract Schedule 2.

The tendered total of the Prices is £100,000.00 excluding VAT.

**Resolving and
avoiding disputes**

The *Representatives* of the *Consultant* are

Address for communications

Address for electronic communications

Address for communications

Address for electronic communications

The *Senior Representatives* of the *Consultant* are

Address for communications

Address for electronic communications

**Option X10
Information
modelling**

If Option X10 is used

**If an *information
execution plan* is to
be identified in the
Contract Data**

The Information Execution Plan identified in the Contract Data is n/a

Option Y(UK)1

Option Y(UK)1 is not used

**Data for the
Schedule of Cost
Components (used
only with Options A
and C)**

The *overhead percentages* for the cost of support people and office overhead are

location

overhead percentage

n/a

**Data for the
Schedule of Cost**

**Components (used
only with Option A)**

The *people rates* are as follows based on 7.5 hour day:

Contract Schedule 1 - The Statement of Requirements and Scope

Digitalisation Pilot to support DWP's Critical Security Infrastructure (CSI)

1. Background to the Client

The Department for Work and Pensions (the **Client**) 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 Client delivers these services across England, Wales and Scotland (including the Orkney and Shetland Islands), across a diverse estate of c.715 buildings. This number is made up primarily of Job Centre Plus offices, which the Client refers to as its 'front-of-house' estate, but also includes Health Assessment Centres and back offices. The back-office sites or 'back-of-house' estate consists of corporate centres, large processing centres and service centres very similar to call centre environments, which are not open to the public. The Client's estate is geographically dispersed due to the high street nature of the Job Centre Plus and Health Assessment Centre portfolio - requiring local presence to serve customers.

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

2. Background to the Client's Requirements

Critical Security Infrastructure (CSI)

The Client's existing electronic security systems have been in place since the early 2000s and are now obsolete, irreparable and do not meet government minimum standards. The systems frequently fail, preventing sites opening and/or creating safety vulnerabilities. The systems also have a short shelf-life as they rely on analogue telephony for communication, which will be withdrawn by the end of 2024. This will render the systems unable to communicate serious incidents off site to enable a proportionate response to take place.

Given the risks this poses to the security of the Client's staff and customer safety, as well as the Client's data and assets, Critical Security Infrastructure (formerly Security Transformation) is a key strategic priority for the Client, forming a major element of the Client's Spending Review (SR) 21 bid. Funding for this programme (in part) was granted as part of the Client's SR21 settlement from HMT.

The CSI programme launched in July 2022 and continues until March 2025, although may run up to March 2026. The expected Capital Works Expenditure is £180m across approximately 605 sites.

CSI Programme

This programme is focused on upgrading and modernisation of security equipment and systems across the Client's estate. The Client's strategy is to reduce the size of the estate by c15% which creates the reduction in the estate to 605. At this time, the reduction is not fully understood against specific sites.

The programme involves replacement/installation and upgrading of security equipment including:

Security Work Required	No of Affected Sites
Automated Access Control Door Full Upgrade (AEGIS – AMAG)	c605
Site Wide Video Surveillance System (VSS) Full Upgrade	c605
Panic Alarm Full Upgrade	c605
IDS Full Upgrade	c605
Key Management Upgrade	c605

Effective delivery of the CSI programme requires multiple commercial solutions to be on boarded at pace to form the "Project Team":

- The Client has appointed Leading Management Services Ltd (LMS) to provide Security Technical Advisor services, providing specialist security advice, design assurance, on site handovers and project sequencing within the supply chain.
- The Client has appointed Mitie FM Ltd (Mitie) and G4S (SS) UK (G4S) to provide elements of the works programme:
 - Mitie will provide the required enabling and building works, with Mitie also providing project coordination and other services to support discharge of the Client's duties as Principal Contractor under the Construction (Design and Management) Regulations 2015 (CDM Regs 2015).

- G4S will supply, install and commission the security components as part of the security contract for the Client and will be the Contractor as defined under The Construction (Design and Management) Regulations 2015 (CDM Regs 2015).
- Del Bosque Ltd has been appointed by the Client as Principal Designer under The CDM Regs 2015 until 31/03/2023, also providing assurance that the Client, through services provided by Mitie, is carrying out all legislative requirements required by the Principal Contractor under The CDM Regs 2015.
- The Client has appointed Perfect Circle JV Ltd to provide programme and commercial management of the programme.

Outside of the Project Team, other support available is as follows:

- Turner and Townsend Project Management Ltd (Turner and Townsend) will support the CSI programme through delivery of the new Estates Programme Management Service (EPMS), which went live on 1st February 2022. Please see more detail in Annex 1.
- The Client's internal information technology team will provide digital infrastructure.

3. The Client's Requirements

a) Requirement

The Client requires a Consultant who can undertake a trial that will support the DWP Estates teams in the delivery of digital plans. The aim is to ensure that the Estates teams will have this information available each time a programme of works is considered.

Following completion of the trial and the findings analysed, DWP Estates and the Commercial Team will investigate a procurement via the existing supply chain.

The trial will undertake 3no surveys and produce BIM models. The following sites have been chosen for the pilot for the reasons set out below which provide a cross section and enable the Department to utilise the benefits offered in 'real time' in order to demonstrate the case for rolling out BIM modelling across the wider estate.

Worcester – a typical medium 'multi floored' site. Preparing a BIM model for this site would enable those works to be planned and costed using the model and would demonstrate the benefits and added value of adopting this approach.

Northampton – a typical medium ‘multi floored’ site. This is the identified trial site for 2 way audio and scheduled to commence on site mid December.

Kidsgrove – a typical small site. This site will be the first completion of the CSI programme so an ideal site to select as an example.

b) Reporting

The Consultant shall provide regular reports and information relating to these services as detailed in this Statement of Requirements and Scope or otherwise required by the Client, the Supply Chain Integrator and the Estates Programme Management Service (EPMS) detailed in Annex 1.

At a minimum, reporting is required to:

- demonstrate whether the approved budget and cash-flow is being maintained; and
- identify those matters which require a decision from the Client and where necessary, provide assistance for the Client to make an informed decision on all such matters.

c) Client Data

Data may be shared with and accessed by the Consultant as part of this contract. All data will have Government Security Classification of OFFICIAL and may also be marked as OFFICIAL-SENSITIVE.

d) Site Visits

Expenses for any necessary site visits are deemed included within the fee proposal and should be limited to the expenses properly spent by the Consultant in providing the Services in line with the Client's Expenses Policy (please see Annex 4).

If required under the latest Government Coronavirus Guidelines, the Client will provide a letter confirming that Consultant personnel undertaking site visits are under contract with the Client and are considered to be key workers.

Consultant Personnel undertaking site visits must comply with the Client's latest coronavirus policies and procedures, minimising contact with others as much as possible.

Consultant Personnel must be fully attuned to the Client's business environment and the sensitive nature of the Client's operations. When conducting site visits, Consultant Personnel must ensure photographs taken do not record identifiable images of other persons or elements of the Client's operations beyond the scope of this Statement of Requirements and Scope.

e) Consultant Personnel Requirements

All *key persons* must be professionally qualified and highly competent in this sector - having relevant technical expertise, qualifications and previous experience in Principal Designer Services.

The Client requires that all Consultant staff 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) and the latest **BS7858 code of practice**.

There is no requirement to apply to the Client 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 and BS7858 checks at no additional charge.

All personnel must comply with the Client's Security Policy (Annex 3). The Consultant will only be expected to comply with those Security Policies and Standards that are applicable to their delivery model and technologies used, which presumes that all Consultant personnel will be using Consultant issued IT equipment and Consultant email addresses.

The Consultant must be able to immediately (on contract award) resource this requirement with Consultant personnel meeting the requirements of this section d).

f) Cooperation, Mobilisation and Handover

The Consultant will be required to work collaboratively with the Client and all members of the Client's supply chain as necessary to support effective delivery of the CSI programme.

Where there is duplication or a potential conflict of interest between the Services provided by the Consultant and the services of another supplier(s), the Consultant shall bring the matter to the attention of the Client as soon as is reasonably practicable, and work in line with the Client's instructions to resolve the service duplication or potential conflict of interest by agreement with the Consultant and the supplier(s) concerned.

The Consultant will provide an effective handover to colleagues in the Client's operations and any other persons identified by the Client. If required, the Consultant will also provide any assistance required by the Client to exit the contract and tender for any ongoing or future support or services free of charge.

Proposal

Please provide a proposal detailing how you will deliver the CSI Digitisation service meeting the Client's requirements. The proposal should include (but not be limited to) the following:

- Details of the key personnel proposed to be used in delivering the services, including rationale for their appointment. The Proposal should include an organogram, whether any of the key personal will be subcontractors, and CVs for those proposed, inclusive of location and grade.
- Timescales to complete this work, specifying any dependencies or potential issues;
- A commercial breakdown of the costs.

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

Within the Department, the Client's Estates 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:

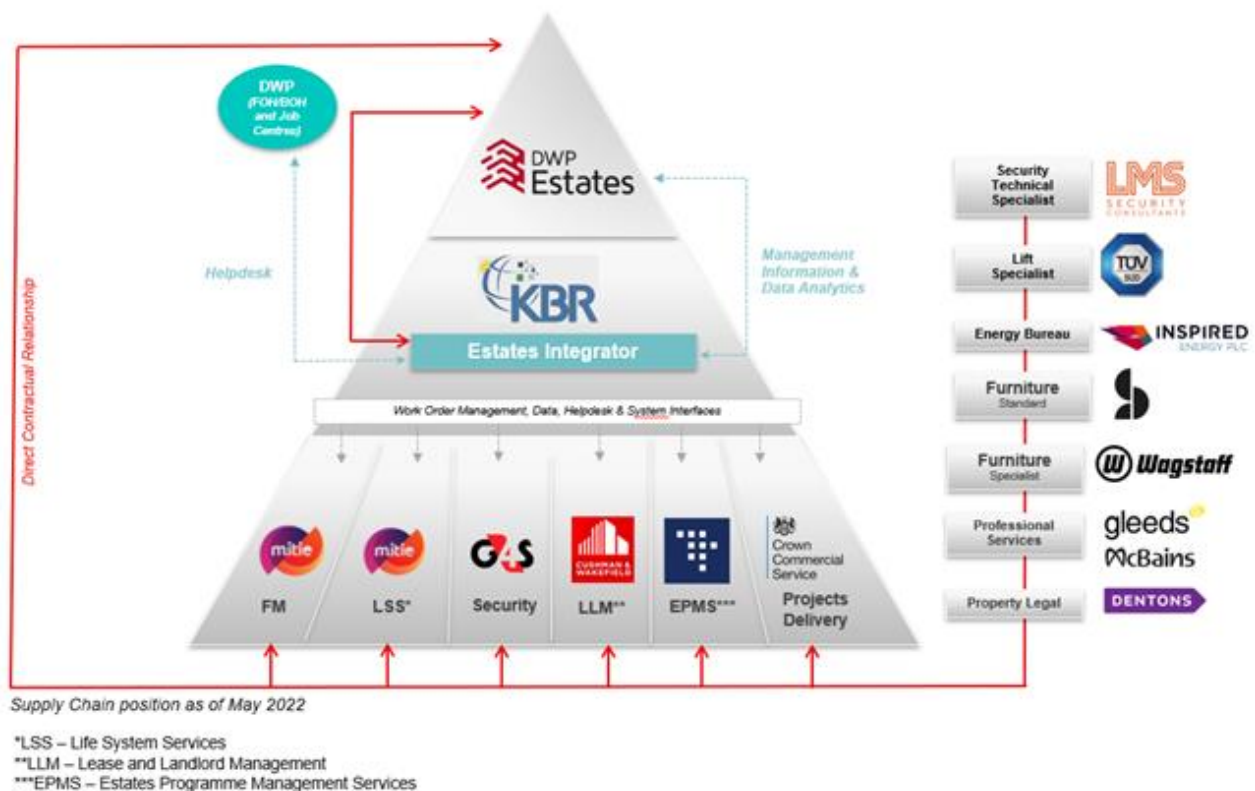
- a) providing a single up-to-date and accurate version of all Client data and information, including a master asset register;
- b) reporting holistically across the Client's estate and estate services;
- c) processing all supply chain invoices for payment;

- 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 Client 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 currently appointed providers of construction professional services listed in Table 2, as well as all providers of construction, fit-out and LCW currently appointed to contracts from the Client’s now-expired ‘Estate Jobcentre & Office Fit Out Contractor Framework,’ as well as 21 providers of construction, fit-out and LCW from the Client’s ‘Taxi Rank Rotational Procedure’ shown in Table 3 and Figure 2 respectively. There is a possibility of future awards to further providers of construction from other public sector Frameworks, including those available from Scape and Pagabo, where the Client deems that the ‘Taxi Rank Rotational Procedure’ is not appropriate. The Projects Delivery supply chain is therefore subject to change.

- **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. The EPMS will provide robust management and oversight across all types of projects for the Client's estate and will be responsible for setting governance, providing robust management information, and oversee cost and risk management for the Client's project pipeline.

Table 2: Summary of the Client's Current Construction Professional Services Providers (currently appointed up to 31st March 2023)

DWP Projects Supported	Supplier	Services	Geographic Area
LCW and minor business as usual projects	McBains Ltd	• Cost Managers	Nationally across England, Wales and Scotland
	Gleeds Advisory Ltd	• Project Managers • Contract Administrators • Principal Designers • Technical Advisors	
Major Capex and WPT projects	Gleeds Advisory Ltd	• Project Managers • Contract Administrators	Nationally across England, Wales and Scotland
	McBains Ltd	• Architects • Building Services Engineer (Mechanical and Electrical Engineers)	Scotland, North-East England, North-West England, Yorkshire and the Humber and East Midlands
	Ridge & Partners LLP	• Civil Engineer • Principal Designer • Building Information Management (BIM) Information Manager • BIM Coordinator • Cost Managers	Wales, West Midlands, East of England, South East, South West and London
Perfect Circle JV Ltd		• WPT Programme Managers and CSI Programme and Commercial Managers	Nationally

The Client's Expenses Policy



Annexure 2 - DWP
Travel Policy2 - Apr 21

Contract Schedule 2 - Activity Schedule

Refer to Contract Schedule 1 - The Statement of Requirements and Scope

Contract Schedule 3 - Consultant Proposal dated 10 November 2022
REDACTED

**Contract Schedule 4 - Government Commercial Function Supplier
Code of Conduct**

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

Contract Schedule 5 - Client Security Policy

SCHEDULE 5 – MINIMUM SECURITY REQUIREMENTS

GENERAL

The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Authority's security requirements as set out in the Contract which include the requirements set out in this Schedule [6] to the Contract (the "**Authority's Security Requirements**"). The Authority's Security Requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Authority Assets, the Authority's Systems Environment and the Contractor's Systems Environment.

Terms used in this Schedule 5 which are not defined below shall have the meanings given to them in clause A1 (Definitions and Interpretations) of the Contract.

1. DEFINITIONS

1.1 In this Schedule 5, the following definitions shall apply:

"Authority Personnel"	shall mean all persons employed by the Authority including directors, officers, employees together with the Authority's servants, agents, consultants, contractors and suppliers but excluding the Contractor and any Sub-contractor (as applicable).
"Availability Test"	shall mean the activities performed by the Contractor to confirm the availability of any or all components of any relevant ICT system as specified by the Authority.
"CHECK"	shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.
"Cloud"	shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data.
"Cyber Essentials"	shall mean the Government-backed, industry-supported scheme managed by the NCSC to help organisations to protect themselves against online threats or the relevant successor or replacement

scheme which is published and/or formally recommended by the NCSC.

“Cyber Security Information Sharing Partnership” or “CiSP”

shall mean the cyber security information sharing partnership established by the NCSC or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.

“Good Security Practice”

shall mean:

- a) the technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for Standardization or the National Institute of Standards and Technology);
- b) security standards and guidelines relating to Information Security (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) provided to the general public or Information Security practitioners and stakeholders by generally recognised authorities and organisations; and
- c) the Government's security policies, frameworks, standards and guidelines relating to Information Security.

“Information Security”

shall mean:

- a) the protection and preservation of:
 - i) the confidentiality, integrity and availability of any Authority Assets, the Authority's Systems Environment (or any part thereof) and the Contractor'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 Authority Assets.
“Information Security Manager”	shall mean the person appointed by the Contractor with the appropriate experience, authority and expertise to ensure that the Contractor complies with the Authority’s Security Requirements.
“Information Security Management System (“ISMS”)	shall mean the set of policies, processes and systems designed, implemented and maintained by the Contractor to manage Information Security Risk as specified by ISO/IEC 27001.
“Information Security Questionnaire”	shall mean the Authority’s set of questions used to audit and on an ongoing basis assure the Contractor’s compliance with the Authority’s Security Requirements.
“Information Security Risk”	shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.
“ISO/IEC 27001, ISO/IEC 27002 and ISO 22301	shall mean a) ISO/IEC 27001; b) ISO/IEC 27002/IEC; and c) ISO 22301 in each case as most recently published by the International Organization for Standardization or its successor entity (the “ISO”) or the relevant successor or replacement information security standard which is formally recommended by the ISO.
“NCSC”	shall mean the National Cyber Security Centre or its successor entity (where applicable).

“Penetration Test”	shall mean a simulated attack on any Authority Assets, the Authority’s Systems Environment (or any part thereof) or the Contractor’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.
“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 Authority Assets, the Authority’s Systems Environment (or any part thereof) or the Contractor’s Systems Environment (or any part thereof).

- 1.2 Reference to any notice to be provided by the Contractor to the Authority shall be construed as a notice to be provided by the Contractor to the Authority’s Representative.

2. PRINCIPLES OF SECURITY

- 2.1 The Contractor shall at all times comply with the Authority’s Security Requirements 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 Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with ISO/IEC 27001 in relation to the Services during the Contract Period.

- 3.2 The Contractor shall appoint an Information Security Manager and shall notify the Authority of the identity of the Information Security Manager on the Commencement Date and, where applicable, within 5 Working Days following any change in the identity of the Information Security Manager.
- 3.3 The Contractor shall ensure that it operates and maintains the Information Security Management System during the Contract 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 Contractor shall provide the Information Security Management System to the Authority upon request within 10 Working Days from such request.

- 3.4 The Contractor 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 Authority.
- 3.5 Notwithstanding the provisions of paragraph **Error! Reference source not found.** to paragraph **Error! Reference source not found.**, the Authority may, in its absolute discretion, notify the Contractor that it is not in compliance with the Authority's Security Requirements and provide details of such non-compliance. The Contractor shall, at its own expense, undertake those actions required in order to comply with the Authority's Security Requirements 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 Authority's Security Requirements within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a Material Breach entitling the Authority to exercise its rights under clause F5.2A.

4. CYBER ESSENTIALS SCHEME

- 4.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, obtain and maintain certification to Cyber Essentials (the "Cyber Essentials Certificate") in relation to the Services during Contract Period. The Cyber Essentials Certificate shall be provided by the Contractor to the Authority annually on the dates as agreed by the Parties.

- 4.2 The Contractor shall notify the Authority 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 Contractor 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 Contract Period after the first date on which the Contractor 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 Material Breach entitling the Authority to exercise its rights under clause F5.2A.

5. RISK MANAGEMENT

- 5.1 The Contractor shall operate and maintain policies and processes for risk management (the **Risk Management Policy**) during the Contract Period which includes standards and processes for the assessment of any potential risks in relation to the Services and processes to ensure that the Authority's Security Requirements are met (the **Risk Assessment**). The Contractor shall provide the Risk Management Policy to the Authority upon request within 10 Working Days of such request. The Authority may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Authority's Security Requirements. The Contractor shall, at its own expense, undertake those actions required in order to implement the changes required by the Authority within one calendar month of such request or on a date as agreed by the Parties.
- 5.2 The Contractor shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Contractor's Systems Environment or in the threat landscape or (iii) at the request of the Authority. The Contractor shall provide the report of the Risk Assessment to the Authority, 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 Contractor shall notify the Authority 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 Authority decides, at its absolute discretion, that any Risk Assessment does not meet the Authority's Security Requirements, the Contractor shall repeat the Risk Assessment within one calendar month of such request or as agreed by the Parties.

- 5.4 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, co-operate with the Authority in relation to the Authority's own risk management processes regarding the Services.
- 5.5 For the avoidance of doubt, the Contractor 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 Contractor 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 Material Breach entitling the Authority to exercise its rights under clause **F5.2A.**

6. SECURITY AUDIT AND ASSURANCE

- 6.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, complete the information security questionnaire in the format stipulated by the Authority (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 Contractor shall conduct Security Tests to assess the Information Security of the Contractor's Systems Environment and, if requested, the Authority's Systems Environment. In relation to such Security Tests, the Contractor 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 Contractor's Systems Environment or in the Authority's System Environment or (iii) at the request of the Authority 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 Authority. The Contractor 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 Contractor 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 Authority in its absolute discretion.
- 6.3 The Authority shall be entitled to send the Authority's Representative to witness the conduct of any Security Test. The Contractor shall provide to the Authority notice of any Security Test at least one month prior to the relevant Security Test.

- 6.4 Where the Contractor provides code development services to the Authority, the Contractor shall comply with the Authority's Security Requirements in respect of code development within the Contractor's Systems Environment and the Authority's Systems Environment.
- 6.5 Where the Contractor provides software development services, the Contractor shall comply with the code development practices specified in the Specification or in the Authority's Security Requirements.
- 6.6 The Authority, or an agent appointed by it, may undertake Security Tests in respect of the Contractor's Systems Environment after providing advance notice to the Contractor. If any Security Test identifies any non-compliance with the Authority's Security Requirements, the Contractor 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 Authority at its absolute discretion. The Contractor shall provide all such co-operation and assistance in relation to any Security Test conducted by the Authority as the Authority may reasonably require.
- 6.7 The Authority shall schedule regular security governance review meetings which the Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, attend.

7. PCI DSS COMPLIANCE AND CERTIFICATION

- 7.1 Where the Contractor obtains, stores, processes or transmits payment card data, the Contractor shall comply with the PCI DSS.
- 7.2 The Contractor 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 Contract Period. The Contractor shall provide the respective PCI Reports to the Authority upon request within 10 Working Days of such request.
- 7.3 The Contractor shall notify the Authority 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 Contractor 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 Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Security Policies and Standards set out Annex A and B.
- 8.2 Notwithstanding the foregoing, the Authority's Security Requirements 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. Where any such change constitutes a Contract Change, any change in the Authority's Security Requirements resulting from such Contract Change (if any) shall be agreed by the Parties in accordance with the Contract Change Procedure. Where any such change constitutes an Operational Change, any change in the Authority's Security Requirements resulting from such Operational Change (if any) shall be agreed by the Parties and documented in the relevant Operational Change Confirmation.
- 8.3 The Contractor shall, and shall procure that any Sub-contractor (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 Supplier may require a nominated representative of the Supplier to join the Cyber Security Information Sharing Partnership on behalf of the Supplier during the Term, in which case the Supplier's nominated representative shall participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.
- 9.2 If the Supplier elects a nominated representative to join the Cyber Security Information Sharing Partnership in accordance with Paragraph 9.1 above, it shall review the NCSC weekly threat reports on a weekly basis and implement recommendations in line with the Supplier's Risk Management Policy.

ANNEX A – AUTHORITY SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

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

- a) Acceptable Use Policy
- b) Information Security Policy
- c) Physical Security Policy
- d) Information Management Policy
- e) Email Policy
- f) Technical Vulnerability Management Policy
- g) Remote Working Policy
- h) Social Media Policy
- i) Forensic Readiness Policy
- j) SMS Text Policy
- k) Privileged Users Security Policy
- l) User Access Control Policy
- m) Security Classification Policy
- n) Cryptographic Key Management Policy
- o) HMG Personnel Security Controls – May 2018
(published on <https://www.gov.uk/government/publications/hmg-personnel-security-controls>)
- p) NCSC Secure Sanitisation of Storage Media (published on <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>) on

ANNEX B – SECURITY STANDARDS

The Security Standards are published on:

<https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards>:

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

Contract Schedule 6 - Key Performance Indicators

Not Used

Contract Schedule 7 - Financial Distress

1. Definitions

1.1. In this Schedule 7 the following definitions apply:

"Credit Rating Threshold" means the minimum credit rating level for the *Consultant* as set out in Annex 1

"Financial Distress Event" means the occurrence or one or more of the events listed in this Schedule 7.

"Financial Distress Service Continuity Plan" means a plan setting out how the *Consultant* will ensure the continued performance in accordance with this contract in the event that a Financial Distress Event occurs;

"Rating Agency" means Fame.

2. Credit rating and duty to notify

2.1. The *Consultant* warrants and represents to the *Client* for the benefit of the *Client* that as at the Contract Date the long-term credit ratings issued for the *Consultant* by the Rating Agency.

2.2. The *Consultant* promptly notifies (or procures that its auditors promptly notify) the *Client* and the *Service Manager* if there is any significant downgrade in the credit rating issued by any Rating Agency for the *Consultant* (and in any event within seven days from the occurrence of the downgrade).

2.3. If there is any downgrade credit rating issued by any Rating Agency for the *Consultant*, the *Consultant* ensures that the *Consultant's* auditors thereafter provide the *Client* or the *Service Manager* within 14 days of a written request by the *Client* or the *Service Manager* with written calculations of the quick ratio for the *Consultant* at such date as may be requested by the *Client* or the *Service Manager*. For these purposes the "quick ratio" on any date means:

Where

A. is the value at the relevant date of all cash in hand and at the bank of the *Consultant*

B. is the value of all marketable securities held by the *Consultant* determined using closing prices on the working day preceding the relevant date

C. is the value at the relevant date of all account receivables of the *Consultant* and

D. is the value at the relevant date of the current liabilities of the *Consultant*.

2.4. The *Consultant*:

- regularly monitors the credit ratings of the *Consultant* with the Rating Agencies and
- promptly notifies (or shall procure that its auditors promptly notify) the *Client* and the *Service Manager* following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, shall ensure that such notification is made within 14 days of the date on which the *Consultant* first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

2.5. For the purposes of determining whether a Financial Distress Event has occurred pursuant to the provisions of paragraph, the credit rating of the *Consultant* shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated the *Consultant* at or below the applicable Credit Rating Threshold.

3. Consequences of a financial distress event

3.1. In the event of:

3.1.1. the credit rating of the *Consultant* dropping below the applicable Credit Rating Threshold;

3.1.2. the *Consultant* issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects;

3.1.3. there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the *Consultant*;

3.1.4. the *Consultant* committing a material breach of covenant to its lenders;

3.1.5. a Subcontractor notifying the *Client* that the *Consultant* has not satisfied any sums properly due for a material specified invoice or sequences of invoices that are not subject to a genuine dispute;

3.1.6. any of the following:

- commencement of any litigation against the *Consultant* with respect to financial indebtedness or obligations under this contract;
- non-payment by the *Consultant* of any financial indebtedness; any financial indebtedness of the *Consultant* becoming due as a result of an event of default
- the cancellation or suspension of any financial indebtedness in respect of the *Consultant* in each case which the *Client* or the *Service Manager* reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of the *Consultant* in accordance with this contract

then, immediately upon notification of the Financial Distress Event (or if the *Client* or the *Service Manager* becomes aware of the Financial Distress Event without notification and brings the event

to the attention of the *Consultant*), the *Consultant* shall have the obligations and the *Client* shall have the rights and remedies as set out in paragraphs 3.2 – 3.6.

3.2. The *Consultant*:

3.2.1 at the request of the *Client* meets the *Client* and the *Service Manager* as soon as reasonably practicable (and in any event within three working days of the initial notification (or awareness) of the Financial Distress Event or such other period as the *Client* or the *Service Manager* may permit and notify to the *Consultant* in writing) to review the effect of the Financial Distress Event on its continued performance in accordance with this contract and

3.2.2. where the *Client* or the *Service Manager* reasonably believes (taking into account any discussions and representations under paragraph 3.2.1) that the Financial Distress Event could impact on the *Consultant's* continued performance in accordance with this Contract:

- submits to the *Client* and the *Service Manager* for approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within 14 days from the initial notification (or awareness) of the Financial Distress Event or such other period as the *Client* or the *Service Manager* may permit and notify to the *Consultant* in writing)
- provides such financial information relating to the *Consultant* as the *Client* or the *Service Manager* may reasonably require.

3.3. The *Client* and the *Service Manager* do not withhold approval of a draft Financial Distress Service Continuity Plan unreasonably. If the *Client* and/or the *Service Manager* do not approve the draft Financial Distress Service Continuity Plan, the *Client* and/or the *Service Manager* inform the *Consultant* of the reasons and the *Consultant* takes those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which the *Consultant* resubmits to the *Client* and the *Service Manager* within seven days of the rejection of the first or subsequent (as the case may be) drafts. This process is repeated until the Financial Distress Service Continuity Plan is approved by the *Client* and/or the *Service Manager* or referred to the dispute resolution procedure.

3.4. If the *Client* and/or the *Service Manager* consider that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not remedy the relevant Financial Distress Event, the *Client* and/or the *Service Manager* may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the dispute resolution procedure.

3.5. Following approval of the Financial Distress Service Continuity Plan by the *Client* or the *Service Manager*, the *Consultant*

- reviews on a regular basis (which shall not be less than monthly) the Financial Distress Service Continuity Plan and assesses whether it remains adequate and up to date to ensure the continued performance in accordance with this contract
- where the Financial Distress Service Continuity Plan is not adequate or up to date in, submits an updated Financial Distress Service Continuity Plan to the *Client* and the *Service Manager* for approval, and the provisions of shall apply to the review and approval process for the updated Financial Distress Service Continuity Plan and
- complies with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).

3.6. Where the *Consultant* reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, the Consultant notifies the *Client* and the *Service Manager* and subject to the agreement of the *Client* and/or the *Service Manager*, the Consultant is relieved of its obligations under paragraph 3.

4. Termination rights

4.1. The *Client* may terminate the *Consultant's* obligation to Provide the Service (which shall take effect as termination under reason R11) if

- the *Consultant* fails to notify the *Client* and the *Service Manager* of a Financial Distress Event in accordance with paragraph 2.2;
- the *Client* and the *Service Manager* fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with paragraph 3 and/or
- the *Consultant* fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with paragraph 3.

5. Primacy of credit ratings

5.1. Without prejudice to the *Consultant's* obligations and the *Client's* rights and remedies under paragraph 3, if, following the occurrence of a Financial Distress Event pursuant to paragraph 2 to the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:

- the *Consultant* is relieved automatically of its obligations under paragraph 3 and
- the *Client* is not entitled to require the Consultant to provide financial information in accordance with paragraph 2.3.

ANNEX 1: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Consultant Credit current rating (long term): Secure

Credit Rating Threshold: Secure

Contract Schedule 8 - GDPR

The following definitions shall apply to this Schedule 8.

Agreement : this contract;

Processor Personnel : means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Agreement

GDPR CLAUSE DEFINITIONS:

Data Protection Legislation : (i) the GDPR, (ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy which, pending a decision from the competent authorities of the EU on the adequacy of the UK data protection regime will include the requirements set out or referenced in Part Three, Title VII, Article 71(1) of the Withdrawal Agreement signed by the UK and the EU in December 2019;

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

Controller , Processor , Data Subject , Personal Data , Personal Data Breach , Data Protection Officer take the meaning given in the Data Protection Legislation.

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

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

DPA 2018 : Data Protection Act 2018

GDPR : the General Data Protection Regulation (Regulation (EU) 2016/679) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

Joint Controllers: where two or more Controllers jointly determine the purposes and means of processing

Protective Measures : appropriate technical and organisational measures which may include: pseudonymisation and/or encryption of Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule 5 - Client Security Policy.

Sub-processor : any third party appointed to process Personal Data on behalf of that Processor related to this Agreement

1. DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the *Client* is the Controller and the *Consultant* is the Processor unless otherwise specified in Schedule

The only processing that the Processor is authorised to do is listed in Schedule 8 by the Controller and may not be determined by the Processor.

1.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

1.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:

- (a) a systematic description of the envisaged processing operations and the purpose of the processing;
- (b) an assessment of the necessity and proportionality of the processing

operations in relation to the *service*;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule 8A, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule X);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this clause;

(B) are subject to appropriate confidentiality undertakings with the Processor or any

Sub- processor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (in accordance with the Data Protection Legislation) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data;

1.5 Subject to clause 1.6, the Processor shall notify the Controller immediately if it:

(a) receives a Data Subject Request (or purported Data Subject Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Data Loss Event.

1.6 The Processor's obligation to notify under clause 1.5 shall include the provision of further information to the Controller in phases, as details become available.

1.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Data Loss Event;

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

1.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(a) the Controller determines that the processing is not occasional;

(b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions

and offences referred to in Article 10 of the GDPR; or

(c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

1.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation .

1.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:

(a) notify the Controller in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 1 such that they apply to the Sub-processor; and

(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

1.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub- processors.

1.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.15 Where the Parties include two or more Joint Controllers as identified in Schedule 8A in accordance with GDPR Article 26, those Parties shall enter into a Joint Controller Agreement based on the terms outlined in Schedule 8 in replacement of Clauses 1.1-

1.14 for the Personal Data under Joint Control.

ANNEX A - PART 2: SCHEDULE OF PROCESSING,

PERSONAL DATA AND DATA SUBJECTS SCHEDULE 8A

PROCESSING, PERSONAL DATA AND DATA SUBJECTS

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

1. The contact details of the Controller's Data Protection Officer are: [To be provided by DWP]
2. The contact details of the Processor's Data Protection Officer are: **REDACTED**,
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

Description	Details
-------------	---------

Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the <i>Client</i> is the Data Controller and the <i>Consultant</i> is the Data Processor.
Subject matter of the processing	The processing is needed in order to ensure that the Data Processor can effectively deliver the Call Off Contract to provide the <i>services</i> to the <i>Client</i> .
Duration of the processing	Personal Data is processed for the duration of the contract to allow <i>services</i> to be performed.
Nature and purposes of the processing	The nature of the processing will include the storage and use of names and business contact details of staff of both the <i>Client</i> and the <i>Consultant</i> as necessary to deliver the services and to undertake contract management. The Contract itself will include the names and business contact details of staff of both the <i>Client</i> and the <i>Consultant</i> involved in delivery or management of the Contract.

Type of Personal Data being Processed	Names, business telephone details and email addresses, office location and position of staff of both the <i>Client</i> and the <i>Consultant</i> .
Categories of Data Subject	Staff of both the <i>Client</i> and the <i>Consultant</i> , including where those staff are named within the Contract itself or involved in contract management.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	Following the <i>completion date</i> , the <i>Consultant</i> will delete the Personal Data from any computers, storage devices and storage media that are to be retained by the Consultant after the expiry of the Contract. The <i>Consultant</i> will certify to the <i>Client</i> that it has completed such deletion.

