Date

18th April 2024

FORM OF AGREEMENT

Incorporating the NEC3 Professional Services Contract April 2013

Between

UK Health Security Agency

And

CBRE Managed Services Limited

For the provision of

Services to carry out the design for a replacement air handling unit at UKHSA RCE Chilton E Block

THIS AGREEMENT BY DEED is made the 18 April 2024

PARTIES:

1. **The Secretary of State for Health and Social Care** (acting as part of the Crown through UK Health Security Agency) with offices at 10 South Colonnade, London, E14 4PU, acting as part of the Crown, (the "***Employer***"); and

2. **CBRE MANAGED SERVICES LIMITED** which is a company incorporated in and in accordance with the laws of England and Wales Company No. 01799580 whose registered office address is at 61 Southwark Street, London, England, SE1 0HL the "***Consultant***").

BACKGROUND

(A) The NHS Shared Business Services, acting as an agent on behalf of its Approved Organisations, (the "**Authority**"), established a framework for Hard Facilities Management services for the benefit of public sector bodies.

(B) The *Consultant* was appointed to the framework and executed the framework agreement (with reference number SBS10166) which is dated 12th April 2022 (the "**Framework Agreement**"). In the Framework Agreement, the Consultant is identified as the "Supplier".

(C) On the 6th November 2023 the *Employer*, acting as part of the Crown, and in the Framework Agreement is identified as a "Contracting Authority" invited the *Consultant* to tender for the *Employer's* hard facilities management requirements in accordance with the Call Off Procedure (as defined in the Framework Agreement).][1]

(D) On the 2nd April 2024 the *Consultant* submitted a tender response and was subsequently selected by the *Employer* to provide the *services*.

(E) The *Consultant* has agreed to Provide the Services in accordance with this agreement and the Framework Agreement.

IT IS AGREED AS FOLLOWS:

1. The *Employer* 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 Services 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 NEC3 Professional Services Contract April 2013 and incorporating the following Options:

   Option A – Priced contract with activity schedule

   W2; Dispute resolution procedure (used in the United Kingdom Housing Grants, Construction and Regeneration Act 1996 applies).

   Option X2, X11 and X18

Option Y(UK)2

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 NEC3 Professional Services Contract April 2013 Edition to "the contract" are references to this contract.

4. This contract and the Framework Agreement is the entire agreement between the parties in relation to the *services* 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 agreement 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 as a deed
EXECUTED AS A DEED by the parties on the date which first appears in this Deed.

EXECUTED AS A DEED by UK Health Security Agency

[redacted]

Full Name: [redacted]

Job Title/Role: [redacted]

Date Signed: 7/5/2024

EXECUTED AS A DEED by CBRE Managed Services Limited ([redacted]

[redacted]

Full Name: [redacted]

Job Title/Role: [redacted]

Date Signed: 03/05/2024

EXECUTED AS A DEED by CBRE Managed Services Limited ([redacted]

[redacted]

Full Name: [redacted]

Job Title/Role: [redacted]

Date Signed: 3/5/24

Professional Services Contract
Contract Data

Part one – Data provided by the *Employer*	
1 General	• The *conditions of contract* are the core clauses and the clauses for main Option A, dispute resolution Option W2 and secondary Options X2, X11, X18, Y(UK)2, and Z of the NEC3 Professional Services Contract (April 2013).
	• The *Employer* is UK Health Security Agency 10 South Colonnade London E14 4PU
	• The *Adjudicator* is the person agreed by the Parties from the list of *Adjudicator*s published by the Chartered Institute of Arbitrators or nominated by the *Adjudicator nominating body* in the absence of agreement.
	• The *services* are to carry out the design for a replacement air handling unit at UKHSA RCE Chilton E Block facility.
	• The Scope is in appendix 2. Final-CBRE-C267106-ChiltonAHUReplaceDesign-App2Scope-V1.0
	• The *language of this 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. • The *period for reply* is two weeks. • The *period for retention* is 12 years following Completion or earlier termination.
	• The *Adjudicator nominating body* is the Royal Institute of Chartered Surveyors • The *tribunal* is arbitration
	• The following matters will be included in the Risk Register 1. Matters raised in initial risk register supplied as part of the

	proposal Final-CBRE-C267106-ChiltonAHUReplaceDesign-App5RiskReg-v1.0. 2. Any and all Matters identified in accordance with Core Clause 15, after the initial risk reduction meeting is held.		
2 The Parties' main responsibilities	• The *Employer* provides access to the following persons, places and things		
	Access to UKHSA RCE Chilton E Block	Access date within one week of contract award date	
3 Time	• *The starting date* is 29th April 2024. • The *Consultant* submits revised programmes at intervals no longer than one month.		
4 Quality	• The quality policy statement and quality plan are provided within 2 weeks of the Contract Date. • The *defects date* is 26 weeks after Completion of the whole of the *services.*		
5 Payment	• The *assessment interval* is one calendar month • The *currency of this contract* is the pound sterling (£). • The *interest rate* is, 2% per annum above the base rate of the Bank of England.		
8 Indemnity, insurance and liability	• The amounts of insurance and the periods for which the *Consultant* maintains insurance are		
	event	**cover**	**Period**
	failure of the *Consultant* to use the skill and care normally used by professionals providing services similar to the *services*	£1,000,000 in respect of each claim and in the aggregate.	from the *starting date* until 12 years following completion of the whole of the *services* or earlier termination
	death of or bodily injury to a person (not an employee of the *Consultant*) or loss of or damage to property resulting	£1,000,000 in respect of each claim and in the aggregate.	from the *starting date* until all notified Defects have been corrected or earlier termination

<table>
<tr><td></td><td>from an action or failure to take action by the Consultant</td><td></td><td></td></tr>
<tr><td></td><td>death of or bodily injury to employees of the Consultant arising out of and in the course of their employment in connection with this contract</td><td>£1,000,000 in respect of each claim and in the aggregate.</td><td>from the starting date until all notified Defects have been corrected or earlier termination</td></tr>
<tr><td></td><td colspan="3">The Consultant's total liability to the Employer for all matters arising under or in connection with this contract, other than the excluded matters, is limited to £1,000,000.</td></tr>
<tr><td>Optional Statements</td><td colspan="3">If the Employer has decided the completion date for the whole of the services
• The completion date for the whole of the services is as per detailed programme Final-CBRE-C267106-ChiltonAHUReplaceDesign-App4Prog-v1.0.
If no programme is identified in part two of the Contract Data – Not Used</td></tr>
<tr><td></td><td colspan="3">If the Employer has identified work which is to meet a stated condition by a key date
• The key dates and conditions to be met from date of appointment are</td></tr>
<tr><td></td><td>Condition to be met
• CBRE Mobilisation
• RIBA 1 Completion
• RIBA 2 Completion
• RIBA 3 Completion
• RIBA 4 Completion</td><td colspan="2">Key Date
29th April 2024
8th May 2024*
7th June 2024*
24th June 2024*
18th July 2024*</td></tr>
<tr><td></td><td colspan="3">*subject to Employer sign off of design. On submission of each RIBA stage – there will be a period of five days for agreement of the drawings for the Consultant to continue with the project development.</td></tr>
<tr><td></td><td colspan="3">If Y(UK)2 is used and the final date for payment is not 14 days after the date when payment is due
• The period for payment is 30 days after receipt of invoice</td></tr>
</table>

	If the *Employer* states any *expenses* – NOT USED
	If the *tribunal* is arbitration • The *arbitration procedure* is the London Court of International Arbitration Rules; • The number of arbitrators shall be one • The place where arbitration is to be held is London • The language to be used in the arbitration proceedings shall be English • If the parties cannot agree the identity of the arbitrator then the nominating body shall be: Royal Institute of Chartered Surveyors
	If Option A is used: • The *Consultant* prepares forecasts of the total *expenses* at intervals no longer than 4 weeks.
Option X1	**Not Used**
Option X2	**If Option X2 is used** • *The law of the project* is the law of England and Wales.
Option X3	**Not Used**
Option X5	**Not Used**
Option X6	**Not Used**
Option X7	**Not Used**
Option X8	**Not Used**
Option X10	**Not Used**
Option X12	**Not Used**
Option X13	**Not Used**
Option X18	**If Option X18 is used** • The *Consultant's* liability to the *Employer* for indirect or consequential loss is limited to nil. • The *Consultant's* liability to the *Employer* for Defects that are not found until after the *defects date* is limited to £1,000,000. • The end of the liability date 1 years after the Completion of the whole of the services.
Option X20	**Not Used**

Option Z	**If Option Z is used** • The *additional conditions of contract* are as detailed in the appended Standard Boiler Plate Amendments.

Part two – Data provided by the *Consultant*

1 Statements given in all contracts	• The *Consultant* is Name: CBRE Managed Services Limited Address: 61 Southwark Street, London, England, SE1 0HL
	• The *key people* are • Name: [redacted] • Job: Head of Projects • Responsibilities Consultant to advise • Experience Consultant to advise • The *staff rates* are as per Final-CBRE-C267106-ChiltonAHUReplaceDesign-App3ActSch-v1.0
	• The following matters will be included in the Risk Register 1. Matters raised in initial risk register supplied as part of the proposal Final-CBRE-C267106-ChiltonAHUReplaceDesign-App5RiskReg-v1.0. 2. Any and all Matters identified in accordance with Core Clause 15, after the initial risk reduction meeting is held.
Optional statements	**If the *Consultant* is to decide the *completion date* for the whole of the *services* – Not Used**
	If the programme is to be identified in the Contract Data As per Final-CBRE-C267106-ChiltonAHUReplaceDesign-App4Prog-v1.0
Include where expenses are being stated by the Consultant	**If the *Consultant* states any *expenses*** • The *expenses* stated by the *Consultant* are as per Final-CBRE-C267106-ChiltonAHUReplaceDesign-App3ActSch-v1.0
	If the *Consultant* requires additional access The *Employer* provides access to the following persons, places and things access to — *access date* UKHSA RCE Chilton — within 1 week of contract award date
	If Option A or C is used • The *activity schedule* is contained within Appendix 3. Final-CBRE-C267106-ChiltonAHUReplaceDesign-App3ActSch-v1.0

	• The tendered total of the Prices is £95,091.00

Appendix 1: Schedule of Amendments to NEC3 Professional Services Contract

Option Z2 - Identified and defined terms

Insert new clause 11.3 additional defined terms.

11.3 (1) Auditor is:

- the *Employer's* internal and external auditors;
- the *Employer'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 *Employer* 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) 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 services, its IPR or its business or which the *Consultant* has indicated to the *Employer* that, if disclosed by the *Employer*, would cause the *Consultant* significant commercial disadvantage or material financial loss.

11.3 (4) Confidential Information is the Employer's Confidential Information and/or the Consultant's Confidential Information.

11.3 (5) 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 *Employer.*

11.3 (6) 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 (7) Crown Body is any department, office or agency of the Crown.

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

11.3 (9) Data Controller has the meaning given to it in the Data Protection Legislation.

11.3 (10) Data Protection Legislation is (i) the GDPR, (ii) the Data Protection Act 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;

11.3 (11) 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 (12) Employer 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 *Employer*, including all IPRs, 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 (13) Employer 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 *Employer*,

• which the *Consultant* is required to generate, process, store or transmit pursuant to this contract or

• any Personal Data for which the *Employer* is the Data Controller to the extent that such Personal Data is held or processed by the *Consultant*.

11 (14) Employer's Premises are premises owned, occupied or leased by the *Employer* and the site of any works to which the *services* relate.

11.3 (15) 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 (16) 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 (17) 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 (18) Halifax Abuse Principle is the principle explained in the CJEU Case C-255/02 Halifax and others.

11.3 (19) 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 (20) 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 (21) 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, 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 (22) Personal Data has the meaning given to it in the Data Protection Legislation.

11.3 (23) Prohibited Act is

- to directly or indirectly offer, promise or give any person working for or engaged by the *Employer* 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 *Employer* 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 (24) 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 (25) 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 (26) Relevant Tax Authority is HM Revenue & Customs, or, if applicable, a tax authority in the jurisdiction in which the *Consultant* is established.

11.3 (27) Security Policy means the *Employer*'s security policy attached as Appendix 1 to Contract Schedule J (Security Provisions) as may be updated from time to time.

11.3 (28) 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 Z4 - Admittance to Employer's Premises

Insert new clause 18A:

18A.1 The *Consultant* submits to the *Employer* details of people who are to be employed by it and its Subconsultants in connection with the *services*. The details include a list of names and addresses, the capabilities in which they are employed, and other information required by the *Employer*.

18A.2 The *Employer* may instruct the *Consultant* to take measures to prevent unauthorised persons being admitted to the Employer's Premises.

18A.3 All of the *Consultant*'s and Subconsultant's people are to carry an *Employer's* pass and comply with all conduct requirements from the *Employer* whilst they are on the parts of the Employer's Premises identified in the Scope.

A.4 The *Consultant* submits to the *Employer* for acceptance a list of the names of the people for whom passes are required. On acceptance, the *Employer* issues the passes to the *Consultant*. Each pass is returned to the *Employer* when the person no longer requires access to that part of the Employer's Premises or after the *Employer* has given notice that the person is not to be admitted to the Employer's Premises.

18A.5 The *Consultant* does not take photographs of the Employer's Premises or of work carried out in connection with the *services* unless it has obtained the acceptance of the *Employer*.

18A.6 The *Consultant* takes the measures needed to prevent its and its Subconsultants' people taking, publishing or otherwise circulating such photographs.

Option Z5 - Prevention of fraud and bribery

Insert new clauses:

17.2.1 The *Consultant* represents and warrants that neither it, nor to the best of its reasonable 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 and/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.

17.2.2 During the carrying out of the *services* the *Consultant* does not

- commit a Prohibited Act and/or
- do or suffer anything to be done which would cause the *Employer* or any of the *Employer'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.

17.2.3 During the carrying out of the *services* the *Consultant*

- establishes, maintains and enforces, and requires that its Subconsultants 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 *Employer* on request and
- provides and maintains and where appropriate enforces an anti-bribery policy (which

shall be disclosed to the *Employer* on request) to prevent it and any *Consultant's* employees or any person acting on the *Consultant's* behalf from committing a Prohibited Act.

17.2.4 The *Consultant* immediately notifies the *Employer* in writing if it becomes aware of any breach of clause 17.2.1, or has reason to believe that it has or any of its employees or Subconsultants 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.

17.2.5 If the *Consultant* makes a notification to the *Employer* pursuant to clause 17.2.4, the *Consultant* responds promptly to the *Employer's* enquiries, co-operates with any investigation, and allows the *Employer* to audit any books, records and/or any other relevant documentation in accordance with this contract.

17.2.6 If the *Consultant* breaches Clause 17.2.3, the *Employer* may by notice require the *Consultant* to remove from carrying out the *services* any *Consultant* employee whose acts or omissions have caused the *Consultant*'s breach.

Option Z6 - Equality and diversity

Insert new clauses:

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 *Employer* reasonably imposes in connection with any equality obligations imposed on the *Employer* at any time under applicable equality Law*;*

27.2 The *Consultant* takes all necessary steps, and informs the *Employer* 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 Z8 – Conflicts of interest

Insert new clauses:

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 *Employer*) 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 *Employer* under this contract.

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

28.3. The *Employer* may terminate the *Consultant's* obligation to Provide the Services immediately under reason R11 and/or to take such other steps the *Employer* deems necessary where, in the reasonable opinion of the *Employer*, 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 *Employer* under this contract.

Option Z9 – Publicity and Branding

Insert new clauses:

29.1 The *Consultant* does not

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

without approval of the *Employer*.

29.2. The *Employer* is entitled to publicise the contract in accordance with any legal obligation upon the *Employer*, 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

Insert new clauses:

26.1 The *Consultant* acknowledges that unless the *Employer* has notified the *Consultant* that the *Employer* is exempt from the provisions of the FOIA, the *Employer* 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 *Employer* so as to enable the *Employer* to comply with its information disclosure obligations.

26.2 The *Consultant*

- transfers to the *Employer* 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 *Employer* with a copy of all information in its possession, or power in the form that the *Employer* requires within five working days (or such other period as the

Employer may specify) of the *Employer's* request,

- provides all necessary assistance as reasonably requested by the *Employer* to enable the *Employer* 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 Subconsultants do likewise.

26.3 The *Employer* 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.

26.4 The *Consultant* does not respond directly to a Request for Information unless authorised to do so by the *Employer*.

26.5 The *Consultant* acknowledges that the *Employer* may, acting in accordance with the Department of Constitutional Affairs' Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000, be obliged to disclose information without consulting or obtaining consent from the *Consultant* or despite the *Consultant* having expressed negative views when consulted.

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

Option Z13 - Confidentiality and Information Sharing

Insert a new clause

26.7 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,

- 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,

26.8 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.

26.9 The *Consultant* may only disclose the Employer Confidential Information to the people who are directly involved in the carrying out of the *services* 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 Employer Confidential Information received otherwise than for the purposes of this contract.

26.10 The *Consultant* may only disclose the Employer 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 *Employer* as the *Employer* 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.

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

26.12 Nothing in this contract shall prevent the *Employer* 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 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 *Employer* 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 *Employer*'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 *Employer* has used its resources,
- for the purpose of the exercise of its rights under this contract or
- to a proposed successor body of the *Employer* 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 *Employer* under this clause 26.12.

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

26.14 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.

26.15 The *Employer* 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 *Employer* (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 J.

Option Z16 - Tax Compliance

Insert new clauses:

26.16 The *Consultant* represents and warrants that at the Contract Date, it has notified the *Employer* 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.

26.17 If, at any point prior to the *defects date*, an Occasion of Tax Non-Compliance occurs, the *Consultant* shall

- notify the *Employer* in writing of such fact within 5 days of its occurrence and
- promptly provide to the *Employer*
    - 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 *Employer* may reasonably require.

Option Z22 - Fair payment

Insert a new clause:

56.1 The *Consultant* assesses the amount due to a Subconsultant without taking into account the amount certified by the *Employer*.

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

- a period for payment of the amount due to the Subconsultant 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 Subconsultant has completed from the previous assessment date up to the current assessment date in this contract,
- a provision requiring the Subconsultant 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 Subconsultant to assess the amount due to a subsubconsultant without taking into account the amount paid by the *Consultant.*

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

Add an additional clause

Y2.5:

Y2.5 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. [Guidance: for services carried out in Northern Ireland]

Option Z44 - Intellectual Property Rights

Delete clause 70 and insert the following clause

In this clause 70 only:

"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 *Employer* 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 *services*. Such licence entitles the *Employer* 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 licencee 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 *Employer* may assign novate or otherwise transfer its rights and obligations under the licence granted pursuant to 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 *Employer*.

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 *Employer* 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 *Employer* in accordance with the foregoing the *Consultant* procures that the third party grants a direct licence to the *Employer* 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 *Employer* or any licensee or assignee of the *Employer*.

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

70.6 The *Consultant* warrants to the *Employer* that it has not granted and shall not (unless authorised by the *Employer*) 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 *Employer* and to the *Employer*'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 services.

70.8 After the termination or conclusion of the *Consultant*'s employment hereunder, the *Consultant* supplies the *Employer* with copies and/or computer discs of such of the Documents

as the *Employer* may from time-to-time request and the *Employer* pays the *Consultant*'s reasonable costs for producing such copies or discs.

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

70.10 The Parties do not disclose information obtained in connection with the *services* except where necessary to carry out their duties under this contract.

Option Z45 – HMRC Requirements

Insert a new clause 18B

This clause is to incorporate HMRC special terms and conditions in the form of HMRC Call-Off Schedule 23 (HMRC Terms) [Guidance: Client to reference Call-Off Schedule 23 (HMRC Terms)].

Option Z47 - Small and Medium Sized Enterprises (SMEs) – Does not apply

Insert new clause:

24.4

The *Consultant* is required to take all reasonable steps to engage SMEs as Subconsultants and to seek to ensure that no less than the percentage of the Subconsultants stated in the Contract Data (the "SME Percentage") are SMEs or that a similar proportion of the *services* is undertaken by SMEs.

The *Consultant* is required to report to the *Employer* in its regular contract management monthly reporting cycle the numbers of SMEs engaged as Subconsultants and the value of the *services* that has been undertaken by SMEs.

Where available, the *Consultant* is required to tender its Subcontracts using the same online electronic portal as was provided by the *Employer* for the purposes of tendering this contract.

The *Consultant* is to ensure that the terms and conditions used to engage Subconsultants are no less favourable than those of this contract. A reason for the *Employer* not accepting subcontract conditions proposed by the *Consultant* is that they are unduly disadvantageous to the Subconsultant.

Option Z48 - Apprenticeships

Insert new clause:

24.5

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

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 delivering the *services,* (which may include support staff and Subconsultants) are provided by employees on formal apprenticeship programmes.

The *Consultant* makes available to its people and Subconsultants 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 carrying out the *services*.

The *Consultant* provides a written 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 *Employer*

- the number of people during the reporting period employed on the contract, including support staff and Subconsultants,
- 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

Insert new clauses:

19 The *Consultant* notifies the *Employer* 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.

90.5 The *Employer* may terminate the *Consultant's* obligation to Provide the Services (which shall take effect as termination under the second bullet point of clause 90.3) 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 *Employer* 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

90.6 The *Employer* may terminate the *Consultant's* obligation to Provide the Service (which shall take effect as termination the second bullet point of clause 90.3) where in the reasonable opinion of the *Employer* 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 Schedule 8 (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

Insert new clauses:

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 *Employer*.

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

    - verify the accuracy of any amounts payable by the *Employer* 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 Subconsultants and any third-party suppliers) in connection with Providing the Services

    - 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 *Employer* has no obligation to inform the *Consultant* of the purpose or objective of its investigations

    - obtain such information as is necessary to fulfil the *Employer'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 *Employer* 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 *Employer* within the scope of the audit

    - reasonable access to sites controlled by the *Consultant* and to any *Consultant's* equipment used to Provide the Services

    - 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 *Employer* for the *Employer'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 Z100 – GDPR

Insert new clause Z100 as follows:

The *Employer* and the *Consultant* shall comply with the provisions of schedule 16

Option Z101 – Cyber Essentials

Insert new clause Z101 as follows:

The *Employer* and the *Consultant* shall comply with the provisions of schedule 18

Option Z102 – Prevention

Add an additional core clause 18.2

18.2 Neither party shall be liable to the other for any failure or delay in performing its obligations under this agreement due to any cause beyond it's reasonable control, including Governmental actions, war, riots, terrorist attacks, civil commotion, fire, flood, epidemic or pandemic (including Covid-19 and any variation or mutation thereof), labour disputes (other than labour disputes involving employees of that party or its sub-contractors' employees) and any act of God. The date for performance of an obligation which has been delayed by such event is to be suspended only for the period of delay caused by the event.

Option Z103 - Working with the Employer and others

Delete clause 23.3 and replace with the following text:

"If the Consultants decides that work does not meet the Condition stated for a Key Date by the date stated and, as a result, the Employer incurs additional cost either in carrying out work or by paying an additional amount to Others in carrying out work on the same project, the additional cost the Employer has paid or will incus is paid by the Consultant. The Employer assesses the additional cost within four weeks of the date when the Condition stated for that Key Date is met. The Employer's right to recover the additional cost is his only right in these circumstances."

Option Z104 – Excluded Matters

Remove bullet 4 of clause 82.1

SCHEDULE 8 FINANCIAL DISTRESS

1. Definitions

1.1. In this Schedule 8 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 8

"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 the rating agency means Dun & Bradstreet.

2. Credit rating and duty to notify

2.1. The *Consultant* warrants and represents to the *Employer* for the benefit of the *Employer* 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 *Employer* 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 *Employer* within 14 days of a written request by the *Employer* with written calculations of the quick ratio for the *Consultant* at such date as may be requested by the *Employer.* 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 *Employer* 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 Subconsultant notifying the *Employer* 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 *Employer* 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 *Employer* 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 *Employer* 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 *Employer* meets the *Employer* 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 *Employer* 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 *Employer* 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 *Employer* 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 *Employer* may permit and notify to the *Consultant* in writing)
- provides such financial information relating to the *Consultant* as the *Employer* may reasonably requires.

3.3. The *Employer* does not withhold approval of a draft Financial Distress Service Continuity Plan unreasonably. If the *Employer* does not approve the draft Financial Distress Service Continuity Plan, the *Employer* informs 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 *Employer* 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 *Employer* or referred to the dispute resolution procedure.

3.4. If the *Employer* considers 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 *Employer* 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*, 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 *Employer* 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 *Employer* and subject to the agreement of the *Employer*, the Consultant is relieved of its obligations under paragraph 3.

4. Termination rights

4.1. The *Employer* may terminate the *Consultant's* obligation to Provide the Services (which shall take effect as termination under the second bullet point of clause 90.3) if

- the *Consultant* fails to notify the *Employer* of a Financial Distress Event in accordance

with paragraph 2.2;

- the *Employer* fails 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 *Employer'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 *Employer* is not entitled to require the *Consultant* to provide financial information in accordance with paragraph 2.3.

SCHEDULE 16 GDPR

The following definitions shall apply to this Schedule 16

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 13 (Security).

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 *Employer* is the Controller and the *Consultant* is the Processor unless otherwise specified in Schedule 16. The only processing that the Processor is authorised to do is listed in Schedule 16 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 *services*;

(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 16, 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 16);

(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 (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 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 16 in accordance with GDPR Article 26, those Parties shall enter into a Joint Controller Agreement based on the terms outlined in Schedule [Y] 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 16 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:
   Office of The Data Protection Officer at DHSC
   Data_protection@dhsc.gov.uk
   Department of Health and Social Care
   1st Floor North
   39 Victoria Street
   London
   SW1H 0EU

2. The contact details of the Processor's Data Protection Officer are: [insert details]

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 *Employer* is the Controller and the *Consultant* is the Processor in accordance with Clause 1.1.
Subject matter of the processing	N/A
Duration of the processing	N/A
Nature and purposes of the processing	N/A

Type of Personal Data being Processed	N/A
Categories of Data Subject	N/A
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	N/A

SCHEDULE 17 SECURITY PROVISIONS

1. CONTRACT SCHEDULE 17 - SECURITY PROVISIONS

1.1 Definitions

For the purposes of this schedule the following terms shall have the meanings given below:

"Affiliates"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;
"Breach of Security"	in accordance with the Security Requirements and the Security Policy, the occurrence of: (a) any unauthorised access to or use of the services the Employer Premises, the Sites, the Consultant System and/or any ICT, information or data (including the Confidential Information and the Employer Data) used by the *Employer* and/or the *Consultant* in connection with this contract; and/or (b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Employer Data), including any copies of such information or data, used by the *Employer* and/or the *Consultant* in connection with this contract.
"Clearance"	means national security clearance and employment checks undertaken by and/or obtained from the Defence Vetting Agency;
“Consulting Equipment”	the hardware, computer and telecoms devices and equipment supplied by the *consultant* or its Subconsultants (but not hired, leased or loaned from the Employer) for the carrying out of the *services*;
"Consultant Software"	software which is proprietary to the *Consultant*, including software which is or will be used by the *Consultant* for the purposes of carrying out of the *services*;
"Consultant System"	the information and communications technology system used by the *Consultant* in carrying out of the *services* including the Software, the Consultant Equipment and related cabling (but excluding the Employer System);
"Control"	means that a person possesses, directly or indirectly, the power to direct or cause the direction of the management and policies of the other person (whether through the

	ownership of voting shares, by contract or otherwise) and "Controls" and "Controlled" shall be interpreted accordingly;
"Default"	any breach of the obligations of the relevant party (including but not limited to fundamental breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant party, its employees, servants, agents or Sub Consultants in connection with or in relation to the subject-matter of this contract and in respect of which such party is liable to the other;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in this contract (if any) or as agreed between the
"Employer Premises"	means premises owned, controlled or occupied by the *Employer* or its Affiliates which are made available for use by the *Consultant* or its Subconsultants for carrying out of the *services* (or any of them) on the terms set out in this contract or any separate agreement or licence;
"Employer System"	the *Employer*'s computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the *Employer* or the *Consultant* in connection with this contract which is owned by or licensed to the *Employer* by a third party and which interfaces with the Consultant System or which is necessary for the *Employer* to receive the *services*;
"Environmental Information Regulations"	the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issues by the Information Commissioner or relevant Government Department in relation to such regulations;
"FOIA"	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 or relevant Government Department in relation to such legislation;
"Good Industry Practice"	the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector;

"ICT"	information and communications technology;
"ICT Environment"	the Employer System and the Consultant System;
"Impact Assessment"	an assessment of a Compensation Event;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Information Assets Register"	the register of information assets to be created and maintained by the *Consultant* throughout the carrying out of the *services* as described in the contract (if any) or as otherwise agreed between the parties;
"ISMS"	the Information Security Management System as defined by ISO/IEC 27001. The scope of the ISMS will be as agreed by the parties and will directly reflect the scope of the *services*;
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the *services* but excluding know how already in the *Consultant*'s or the *Employer*'s possession before this contract;
"List x"	means, in relation to a Subconsultant, one who has been placed on List x in accordance with Ministry of Defence guidelines and procedures, due to that Sub Consultant undertaking work on its premises marked as CONFIDENTIAL or above;
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"Process"	has the meaning given to it under the Data Protection Legislation but, for the purposes of this contract, it shall include both manual and automatic processing;
"Protectively Marked"	shall have the meaning as set out in the Security Policy Framework.
"Regulatory Bodies"	those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this contract or any other affairs of the *Employer* and "Regulatory Body" shall be construed accordingly;

"Request for Information"	a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Regulations;
"Security Management Plan"	the *Consultants* security plan prepared pursuant to paragraph 1.5.3 of schedule J (Security Management Plan) an outline of which is set out in Appendix 1 of schedule J (Security Management Plan);
"Security Policy Framework"	means the Cabinet Office Security Policy Framework (available from the Cabinet Office Security Policy Division);
"Security Requirements"	means the requirements in the contract relating to security of the carrying out of the *services* (if any) or such other requirements as the *Employer* may notify to the *Consultant* from time to time;
"Security Tests"	shall have the meaning set out in Appendix 2 (Security Management Plan)
"Software"	Specially Written Software, *Consultant* Software and Third-Party Software;
"Specially Written Software"	any software created by the *Consultant* (or by a third party on behalf of the *Consultant*) specifically for the purposes of this contract;
"Staff Vetting Procedures"	the *Employer's* procedures and departmental policies for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures, including, but not limited to, the provisions of the Official Secrets Act 1911 to 1989;
"Statement of Applicability"	shall have the meaning set out in ISO/IEC 27001 and as agreed by the parties during the procurement phase;
"Standards"	the British or international standards, *Employer*'s internal policies and procedures, Government codes of practice and guidance together with any other specified policies or procedures referred to in this contract (if any) or as otherwise agreed by the parties;
"Third Party Software"	software which is proprietary to any third party other than an Affiliate of the *Consultant* which is or will be used by the *Consultant* for the purposes of carrying out of the *services.*

1.2 Introduction

1.2.1 This schedule covers:

1.2.1.1 principles of protective security to be applied in carrying out of the *services*;

1.2.1.2 wider aspects of security relating to carrying out of the *services*;

1.2.1.3 the development, implementation, operation, maintenance and continual improvement of an ISMS;

1.2.1.4 the creation and maintenance of the Security Management Plan;

1.2.1.5 audit and testing of ISMS compliance with the Security Requirements;

1.2.1.6 conformance to ISO/IEC 27001 (Information Security Requirements Specification) and ISO/IEC27002 (Information Security Code of Practice) and;

1.2.1.7 obligations in the event of actual, potential or attempted breaches of security.

1.3 Principles of Security

1.3.1 The *Consultant* acknowledges that the *Employer* places great emphasis on the confidentiality, integrity and availability of information and consequently on the security provided by the ISMS.

1.3.2 The *Consultant* shall be responsible for the effective performance of the ISMS and shall at all times provide a level of security which:

1.3.2.1 is in accordance with Good Industry Practice, the *law of the contract* and this contract;

1.3.2.2 complies with the Security Policy;

1.3.2.3 complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) available from the Cabinet Office Security Policy Division (COSPD);

1.3.2.4 meets any specific security threats to the ISMS; and

1.3.2.5 complies with ISO/IEC27001 and ISO/IEC27002 in accordance with paragraph 1.3.2 of this schedule;

1.3.2.6 complies with the Security Requirements; and

1.3.2.7 complies with the *Employer*'s ICT standards.

1.3.3 The references to standards, guidance and policies set out in paragraph 1.3.2.2 shall be deemed to be references to such items as developed and

updated and to any successor to or replacement for such standards, guidance and policies, from time to time.

1.3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the *Consultant* gives an early warning to the *Employer* of such inconsistency immediately upon becoming aware of the same, and the *Employer* shall, as soon as practicable, advise the *Consultant* which provision the *Consultant* shall be required to comply with.

1.4 ISMS and Security Management Plan

1.4.1 Introduction:

(i) The *Consultant* shall develop, implement, operate, maintain and continuously improve and maintain an ISMS which will, without prejudice to paragraph 1.3.2, be accepted, by the *Employer*, tested in accordance with the provisions relating to testing as set out in the contract (if any) or as otherwise agreed between the Parties, periodically updated and audited in accordance with ISO/IEC 27001.

1.4.1.1 The *Consultant* shall develop and maintain a Security Management Plan in accordance with this Schedule to apply during the carrying out of the *services*.

1.4.1.2 The *Consultant* shall comply with its obligations set out in the Security Management Plan.

1.4.1.3 Both the ISMS and the Security Management Plan shall, unless otherwise specified by the *Employer*, aim to protect all aspects of the *services* and all processes associated with carrying out of the *services*, including the construction, use, alterations or demolition of the *services*, the Consultant System and any ICT, information and data (including the Employer Confidential Information and the Employer Data) to the extent used by the *Employer* or the *Consultant* in connection with this contract.

1.4.2 Development of the Security Management Plan:

1.4.2.1 Within 20 Working Days after the Contract Date and in accordance with paragraph 1.4.4 (Amendment and Revision), the *Consultant* will prepare and deliver to the *Employer* for acceptance a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan set out in Appendix 2 of this Part 2 of this Contract Schedule J.

1.4.2.2 If the Security Management Plan, or any subsequent revision to it in accordance with paragraph 1.4.4 (Amendment and Revision), is accepted by the *Employer* it will be adopted immediately and will replace the previous version of the Security Management Plan at Appendix 2 of this Part 2 of this Contract

Schedule J. If the Security Management Plan is not accepted by the *Employer* the *Consultant* shall amend it within 10 Working Days or such other period as the parties may agree in writing of a notice of non-acceptance from the *Employer* and re-submit to the *Employer* for acceptance. The parties will use all reasonable endeavours to ensure that the acceptance process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the parties may agree in writing) from the date of its first submission to the *Employer*. If the *Employer* does not accept the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. No acceptance to be given by the *Employer* pursuant to this paragraph 1.4.2.2 of this schedule may be unreasonably withheld or delayed. However any failure to accept the Security Management Plan on the grounds that it does not comply with the requirements set out in paragraph 1.4.3.4 shall be deemed to be reasonable.

1.4.3 Content of the Security Management Plan:

1.4.3.1 The Security Management Plan will set out the security measures to be implemented and maintained by the *Consultant* in relation to all aspects of the *services* and all processes associated with carrying out of the *services* and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the *services* comply with the provisions of this schedule (including the principles set out in paragraph 1.3);

1.4.3.2 The Security Management Plan (including the draft version) should also set out the plans for transiting all security arrangements and responsibilities from those in place at the Contract Date to those incorporated in the *Consultant*'s ISMS at the date notified by the *Employer* to the *Consultant* for the *Consultant* to meet the full obligations of the Security Requirements.

1.4.3.3 The Security Management Plan will be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other schedules of this contract which cover specific areas included within that standard.

1.4.3.4 The Security Management Plan shall be written in plain English in language which is readily comprehensible to the staff of the *Consultant* and the *Employer* engaged in the *services* and shall only reference documents which are in the possession of the *Employer* or whose location is otherwise specified in this schedule.

1.4.4 Amendment and Revision of the ISMS and Security Management Plan:

1.4.4.1 The ISMS and Security Management Plan will be fully reviewed and updated by the *Consultant* annually or from time to time to reflect:

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Consultant System, the *services* and/or associated processes;

(c) any new perceived or changed security threats; and

(d) any reasonable request by the *Employer*.

1.4.4.2 The *Consultant* will provide the *Employer* with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the *Employer*. The results of the review should include, without limitation:

(a) suggested improvements to the effectiveness of the ISMS;

(b) updates to the risk assessments;

(c) proposed modifications to the procedures and controls that effect information security to respond to events that may impact on the ISMS; and

(d) suggested improvements in measuring the effectiveness of controls.

1.4.4.3 On receipt of the results of such reviews, the *Employer* will accept any amendments or revisions to the ISMS or Security Management Plan in accordance with the process set out at paragraph 1.4.2.2.

1.4.4.4 Any change or amendment which the *Consultant* proposes to make to the ISMS or Security Management Plan (as a result of an *Employer's* request or change to the *services* or otherwise) shall be subject to the early warning procedure and shall not be implemented until accepted in writing by the *Employer*.

1.4.5 Testing

1.4.5.1 The *Consultant* shall conduct Security Tests of the ISMS on an annual basis or as otherwise agreed by the parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the *Employer.*

1.4.5.2 The *Employer* shall be entitled to witness the conduct of the Security Tests. The *Consultant* shall provide the *Employer* with the results of such tests (in a form accepted by the *Employer* in

advance) as soon as practicable after completion of each Security Test.

1.4.5.3 Without prejudice to any other right of audit or access granted to the *Employer* pursuant to this contract, the *Employer* and/or its authorised representatives shall be entitled, at any time and without giving notice to the *Consultant*, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the *Consultant*'s compliance with the ISMS and the Security Management Plan. The *Employer* may notify the *Consultant* of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the carrying out of the *services*. If such tests adversely affect the *Consultant*'s ability to carry out the *services* in accordance with the Scope, the *Consultant* shall be granted relief against any resultant under-performance for the period of the tests.

1.4.5.4 Where any Security Test carried out pursuant to paragraphs 1.4.5.2 or 1.4.5.3 above reveals any actual or potential Breach of Security, the *Consultant* shall promptly notify the *Employer* of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the *Consultant* proposes to make in order to correct such failure or weakness. Subject to the *Employer*'s acceptance in accordance with paragraph (i), the *Consultant* shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the *Employer* or, otherwise, as soon as reasonably possible. Where the change to the ISMS or Security Management Plan is made to address a non-compliance with the Security Policy or Security Requirements, the change to the ISMS or Security Management Plan is Disallowed Cost.

1.5 Compliance with ISO/IEC 27001

1.5.1 Unless otherwise agreed by the parties, the *Consultant* shall obtain independent certification of the ISMS to ISO/IEC 27001 within 12 months of the Contract Date and shall maintain such certification until the Defects Certificate or a termination certificate has been issued.

1.5.2 In the event that paragraph 1.5.1 above applies, if certain parts of the ISMS do not conform to Good Industry Practice, or controls as described in ISO/IEC 27002 are not consistent with the Security Policy, and, as a result, the *Consultant* reasonably believes that it is not compliant with ISO/IEC 27001, the *Consultant* shall promptly notify the *Employer* of this and the *Employer* in its absolute discretion may waive the requirement for certification in respect of the relevant parts.

1.5.3 The *Employer* shall be entitled to carry out such regular security audits as may be required and in accordance with Good Industry Practice, in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001.

1.5.4 If, on the basis of evidence provided by such audits, it is the *Employer*'s reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the *Consultant*, then the *Employer* shall notify the *Consultant* of the same and give the *Consultant* a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to become compliant with the principles and practices of ISO/IEC 27001. If the *Consultant* does not become compliant within the required time then the *Employer* has the right to obtain an independent audit against these standards in whole or in part.

1.5.5 If, as a result of any such independent audit as described in paragraph 1.5.4 the *Consultant* is found to be non-compliant with the principles and practices of ISO/IEC 27001 then the *Consultant* shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the *Employer* in obtaining such audit.

1.6 Breach of Security

1.6.1 Either party shall give an early warning to the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

1.6.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 1.6.1, the *Consultant* shall:

1.6.2.1 immediately take all reasonable steps necessary to:

(a) remedy such breach or protect the integrity of the ISMS against any such potential or attempted breach or threat; and

(b) prevent an equivalent breach in the future.

such steps shall include any action or changes reasonably required by the *Employer*; and

1.6.2.2 as soon as reasonably practicable provide to the *Employer* full details (using such reporting mechanism as defined by the ISMS) of the Breach of Security or the potential or attempted Breach of Security.

Appendix 1 – Security Policy

Appendix 2 – Security Management Plan

SCHEDULE 18 CYBER ESSENTIALS

CYBER ESSENTIALS SCHEME

1. DEFINITIONS

1.1 In this Schedule, the following words shall have the following meanings:

"Cyber Essentials Scheme"	the Cyber Essentials Scheme developed by the Government which provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats (as may be amended from time to time). Details of the Cyber Essentials Scheme can be found here: https://www.ncsc.gov.uk/cyberessentials/overview;
"Cyber Essentials Basic Certificate"	the certificate awarded on the basis of self-assessment, verified by an independent certification body, under the Cyber Essentials Scheme and is the basic level of assurance;
"Cyber Essentials Certificate"	Cyber Essentials Basic Certificate, the Cyber Essentials Plus Certificate or the Cyber Essential Scheme certificate equivalent to be provided by the *Consultant* as set out in the Framework Data Sheet;
"Cyber Essential Scheme Data"	sensitive and personal information and other relevant information as referred to in the Cyber Essentials Scheme; and
"Cyber Essentials Plus Certificate"	the certification awarded on the basis of external testing by an independent certification body of the *Consultant's* cyber security approach under the Cyber Essentials Scheme and is a more advanced level of assurance.

2. CYBER ESSENTIALS OBLIGATIONS

2.1 Where the Scope requires that the *Consultant* provide a Cyber Essentials Certificate prior to the execution of the *services* the *Consultant* shall provide a valid Cyber Essentials Certificate, then on or prior to the commencement of the *services* the *Consultant* delivers to the *Employer* evidence of the same. Where the *Consultant* fails to comply with this paragraph it shall be prohibited from commencing the carrying out of the *services* under any contract until such time as the *Consultant* has evidenced to the *Employer* its compliance with this paragraph 2.1.

2.2 Where the *Consultant* continues to Process Cyber Essentials Scheme Data during the carrying out of the *services* the *Consultant* delivers to the *Employer* evidence of renewal of the Cyber Essentials Certificate on each anniversary of the first applicable certificate obtained by the *Consultant* under paragraph 2.1.

2.3 Where the *Consultant* is due to Process Cyber Essentials Scheme Data after the commencement of the *services* but before completion of the *services* the *Consultant* delivers to the *Employer* evidence of:

2.3.1 a valid and current Cyber Essentials Certificate before the *Consultant* Processes any such Cyber Essentials Scheme Data; and

2.3.2 renewal of the valid Cyber Essentials Certificate on each anniversary of the first Cyber Essentials Scheme certificate obtained by the *Consultant* under paragraph 2.1.

2.4 In the event that the *Consultant* fails to comply with paragraphs 2.2 or 2.3 (as applicable), the *Employer* reserves the right to terminate this contract for material Default.

2.5 The *Consultant* ensures that all sub-contracts with Sub-Consultants who Process Cyber Essentials Data contain provisions no less onerous on the Sub-Consultants than those imposed on the *Consultant* under this contract in respect of the Cyber Essentials Scheme under paragraph 2.1 of this Schedule

2.6 This Schedule shall survive termination or expiry of this contract.

Appendix	File Name
2. Scope	Final-CBRE-C238425-LeedsRoofReplaceDesign-App2Scope-v1.0
3. Activity Schedule	Final-CBRE-C238425-LeedsRoofReplaceDesign-App3ActSch-v1.0
4. Project Programme	Final-CBRE-C238425-LeedsRoofReplaceDesign-App4Prog-v1.0
5. Risk Register	Final-CBRE-C238425-LeedsRoofReplaceDesign-App5RiskReg-v1.0
6. Work Method	Final-CBRE-C238425-LeedsRoofReplaceDesign-App6Proposal-v1.0
7. Project RIBA Stages	Final-CBRE-C238425-LeedsRoofReplaceDesign-App7RIBAStages-v1.0
8. Project Organogram	Final-CBRE-C238425-LeedsRoofReplaceDesign-App8Organogram-v1.0