

---

# STANDARD 'BOILERPLATE' AMENDMENTS

---

NEC / JCT / PPC2000

NOVEMBER 15, 2018  
CABINET OFFICE  
Crown Commercial Service

## Table of Contents

<b>NEC 3 / NEC 4</b>	4
Definitions	4
Admittance to Site	8
Prevention of Fraud and Bribery	8
Official Secrets	9
Freedom of Information	10
Confidentiality and Information Sharing	11
Security Requirements	13
Tax Compliance	13
Project Bank Accounts	14
Fair Payment	14
Building Information Modelling (BIM)	15
The Housing Grants, Construction and Regeneration Act 1996	15
Intellectual Property Rights	15
MOD DEFCONS	17
Small and Medium Enterprises (SMEs)	17
Apprenticeships	18
GDPR	19
Cyber Essentials	19
<b>Schedules</b>	
GDPR	20
Security Provisions	27
Cyber Essentials	37
<b>JCT design and build contract 2016 edition</b>	
<b>JCT standard building contract with quantities 2016 edition/without quantities edition</b>	
<b>JCT intermediate building contract with contractor's design 2016 design, intermediate building contract 2016 edition</b>	39
Definitions	40
Contracts and Rights of Third Parties Act 1999	43
MOD DEFCONS Requirements	43
Freedom of Information	44

Tax Compliance .....	44
GDPR .....	45
Confidentiality and Information Sharing.....	45
Prevention of Fraud and Bribery.....	47
Security Requirements.....	48
Cyber Essentials .....	48
Admittance to the site .....	48
Legislation and Official Secrets .....	49
Building Information Modelling (BIM) .....	49
Copyright and use / Intellectual Property Rights.....	49
Conditions of Sub-contracting .....	51
Apprenticeships .....	51
Project Bank Accounts (inc. Schedule).....	52
<b>Schedules</b>	
GDPR .....	60
Security Provisions .....	66
Cyber Essentials .....	76
<b>JCT Minor Works with Contractor Design/ without Contractor Design .....</b>	<b>78</b>
Definitions .....	78
Contracts and Rights of Third Parties Act 1999 .....	81
MOD DEFCONS Requirements .....	81
Freedom of Information .....	81
Tax Compliance .....	82
GDPR .....	83
Confidentiality and Information Sharing.....	83
Prevention of Fraud and Bribery.....	85
Security Requirements.....	86
Cyber Essentials .....	86
Admittance to the site .....	86
Legislation and Official Secrets .....	87
Building Information Modelling (BIM) .....	87
Copyright and use / Intellectual Property Rights.....	87

Conditions of Sub-contracting .....	89
Apprenticeships .....	89
Project Bank Accounts (inc. Schedule) .....	90
<b>Schedules</b>	
GDPR .....	98
Security Provisions .....	104
Cyber Essentials .....	115
<b>PPC2000</b> .....	<b>117</b>
Definitions .....	117
Contracts and Rights of Third Parties Act 1999 .....	120
MOD DEFCONS Requirements .....	120
Freedom of Information .....	120
Tax Compliance .....	121
GDPR .....	121
Confidentiality and Information Sharing.....	121
Prevention of Fraud and Bribery.....	123
Security Requirements.....	124
Cyber Essentials .....	124
Admittance to the site .....	125
Legislation and Official Secrets .....	125
Copyright and use / Intellectual Property Rights.....	125
Conditions of Sub-contracting .....	127
Project Bank Accounts .....	128
Building Information Modelling (BIM) .....	134
Apprenticeships .....	134
GDPR .....	136
Security Provisions .....	142
Cyber Essentials .....	154

## SCHEDULE OF AMENDMENTS TO NEC3 / NEC4 ENGINEERING AND CONSTRUCTION CONTRACT

### Interpretation Table

Where these Z Clauses are used for the NEC3 Contract rather than the NEC4 Contract the following interpretation table shall apply:

Defined term in below Z clauses	Replacement defined term for use with NEC3
<i>Client</i>	<i>Employer</i>
Scope	Works Information
Clause number(s) in below Z clauses	Replacement clause number(s) for use with NEC3
18.4	18.2
20.5 to 20.7 (inclusive)	20.6-20.8 (inclusive)
29.3-29.19 (inclusive)	28.1-28.17 (inclusive)
57	56
Y2.6	Y2.5

In addition, where there are alternative clauses to be used for the NEC3 and the NEC4 they are expressly shown below.

Option Y(UK)3: The Contracts (Rights of Third Parties) Act 1999 [NEC4 only]

Z20.1 In clause Y3.2 delete "Other" and replace with:

Y3.2: 'Subject to the express rights of any person under any *collateral warranty arrangement* granted under the provisions of this contract and other'

Option Y(UK)3: The Contracts (Rights of Third Parties) Act 1999 [NEC3 only]

Z20.1 In clause Y3.1 delete "A" and replace with:

Y3.1: 'Subject to the express rights of any person under any *collateral warranty arrangement* granted under the provisions of this contract, a"

## Option Z2 Identified and defined terms

Insert new clause 11.3 additional defined terms

11.3 (1) *Client Confidential Information* is all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and contractors of the *Client*, 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 (2) *Client Data* is

- the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:
- supplied to the *Contractor* by or on behalf of the *Client*; or
- which the *Contractor* is required to generate, process, store or transmit pursuant to this contract; or

any Personal Data for which the *Client* is the Data Controller to the extent that such Personal Data is held or processed by the Contractor

11 (3) Commercially Sensitive Information is the information agreed between the parties (if any) comprising the information of a commercially sensitive nature relating to the *Contractor*, the charges for the works, its IPR or its business or which the *Contractor* has indicated to the *Client* that, if disclosed by the *Client*, would cause the *Contractor* significant commercial disadvantage or material financial loss;

11.3 (4) Confidential Information is the *Client's* Confidential Information and/or the *Contractor'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 *Client*.

11.3 (6) Contractor's Confidential Information is any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and contractors of the *Contractor*, 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) Data Controller has the meaning given to it in the Data Protection Act 2018

11.3 (9) 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 (10) 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(11) 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 (12) General Anti-Abuse Rule is:

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

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

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

(a) 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;

(b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and

(c) all other rights having equivalent or similar effect in any country or jurisdiction;

11.3 (15) 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 *Contractor* is bound to comply;

11.3(16) An Occasion of Tax Non-Compliance is:

- where any tax return of the *Contractor* 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 *Contractor* 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;
- The failure of an avoidance scheme which the *Contractor* was involved in, and which was, or should have been, notified to a Relevant Tax Authority under DOTAS or any equivalent or similar regime; and/or

where any tax return of the *Contractor* 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(17) Personal Data has the meaning given to it in the Data Protection Act 2018

11.3 (18) Prohibited Act is:

- to directly or indirectly offer, promise or give any person working for or engaged by the *Client* y or other Contracting Body or any other public body a financial or other advantage to:
  - induce that person to perform improperly a relevant function or activity; or
  - reward that person for improper performance of a relevant function or activity;
- to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this contract;
- committing any offence:
  - under the Bribery Act 2010 (or any legislation repealed or revoked by such Act)
  - under legislation or common law concerning fraudulent acts; or
  - defrauding, attempting to defraud or conspiring to defraud the *Client*; or

any activity, practice or conduct which would constitute one of the offences listed above if such activity, practice or conduct had been carried out in the UK.

11.3 (19) 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 (20) 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 (21) Relevant Tax Authority is HM Revenue & Customs, or, if applicable, a tax authority in the jurisdiction in which the *Contractor* is established.

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



## Option Z 4

### Admittance to *site*

Insert new clause 19A:

19A.1 The *Contractor* submits to the *Project Manager* details of people who are to be employed by it and its Subcontractors in connection with the *works*. The details include a list of names and addresses, the capabilities in which they are employed, and other information required by the *Project Manager*.

19A.2 The *Project Manager* may instruct the *Contractor* to take measures to prevent unauthorised persons being admitted to *site*. The instruction is a compensation event if the measures are additional to those required by the *Scope*.

19A.3 Employees of the *Contractor* and its Subcontractors are to carry a *Client's* pass and comply with all conduct requirements from the *Client* whilst they are on the parts of the *site* identified in the *Scope*.

19A.4 The *Contractor* submits to the *Project Manager* for acceptance a list of the names of the people for whom passes are required. On acceptance, the *Project Manager* issues the passes to the *Contractor*. Each pass is returned to the *Project Manager* when the employee no longer requires access to that part of the *site* or after the *Project Manager* has given notice that the employee is not to be admitted to the *site*.

19A.5 The *Contractor* does not take photographs of the *site* or of work carried out in connection with the *works* unless it has obtained the acceptance of the *Project Manager*.

19A.6 The *Contractor* takes the measures needed to prevent its and its Subcontractors' people taking, publishing or otherwise circulating such photographs.

## Option Z5      Prevention of fraud and bribery

Insert new clauses:

18.4.1 The *Contractor* represents and warrants that neither it, nor to the best of its knowledge any of its employees, 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.

18.4.2 During the carrying out of the *works* the *Contractor* does not:

- commit a Prohibited Act; and/or
- do or suffer anything to be done which would cause the *Client* or any of the *Client's* employees,

consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements

18.4.3 During the carrying out of the *works* the *Contractor*:

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

18.4.4 The *Contractor* immediately notifies the *Client* in writing if it becomes aware of any breach of clause 18.4.1, or has reason to believe that it has or any of its employees or Subcontractors have:

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

18.4.5 If the *Contractor* makes a notification to the *Client* pursuant to clause 18.4.4, the *Contractor* responds promptly to the *Client's* enquiries, co-operates with any investigation, and allows the *Client* to audit any books, records and/or any other relevant documentation in accordance with this contract.

18.4.6 If the *Contractor* breaches Clause 18.4.3, the *Client* may by notice require the *Contractor* to remove from carrying out the *works* any *Contractor* employee whose acts or omissions have caused the *Contractor's* breach.

**Option Z 7**

**Legislation and Official secrets**

Insert new clauses:

20.5 The *Contractor* complies with Law in the carrying out of the *works*.

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

20.7 The *Contractor* notifies its employees and its Subcontractors of their duties under these Acts.

## Option Z 10

### Freedom of information

Insert new clauses:

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

29.4 The *Contractor*:

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

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

29.6 The *Contractor* does not respond directly to a Request for Information unless authorised to do so by the *Project Manager*.

29.7 The *Contractor* acknowledges that the *Client* 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 *Contractor* or despite the *Contractor* having expressed negative views when consulted.

29.8 The *Contractor* ensures that all Information is retained for disclosure throughout the *period for retention* and permits the *Project Manager* to inspect such records as and when reasonably requested from time to time.

## Option Z 13

### Confidentiality and Information Sharing

Insert a new clause

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

29.10 The clause above shall not apply to the extent that:

- such disclosure is a requirement of the *law of the contract* 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.

29.11 The *Contractor* may only disclose the *Client's* Confidential Information to the Contractor Personnel who are directly involved in the carrying out of the *works* and who need to know the information, and shall ensure that such Contractor Personnel are aware of and shall comply with these obligations as to confidentiality.

The *Contractor* shall not, and shall procure that the Contractor Personnel do not, use any of the *Client* Confidential Information received otherwise than for the purposes of this contract.

29.12 The *Contractor* may only disclose the *Client* Confidential Information to the Contractor Personnel who need to know the information, and shall ensure that such Contractor Personnel 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 Contractor Personnel causes or contributes (or could cause or contribute) to the *Contractor* breaching its obligations as to confidentiality under or in connection with this contract, the *Contractor* 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 Contractor Personnel, the *Contractor* shall provide such evidence to the *Client* as the *Client* may reasonably require (though not so as to risk compromising or prejudicing the case) to demonstrate that the *Contractor* is taking appropriate steps to comply with this clause, including copies of any written communications to and/or from Contractor Personnel, and any minutes of meetings and any other records which provide an audit trail of any discussions or exchanges with Contractor Personnel in connection with obligations as to confidentiality.

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

29.14 Nothing in this contract shall prevent the *Client* from disclosing the *Contractor'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 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 any consultant, contractor or other person engaged by the *Client* or any person conducting an Office of Government Commerce gateway review;
- for the purpose of the examination and certification of the *Client's* accounts; or
- for any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the *Client* has used its resources.

and for the purposes of the foregoing, disclosure of the Contractor's Confidential Information shall be on a confidential basis and subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Client under this clause 29.14.

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

29.16 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

29.17 The *Client* may disclose the Confidential Information of the *Contractor*:

- on a confidential basis to any Crown Body for any proper purpose of the *Client* or the relevant Crown Body;
- to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;
- to the extent that the *Client* (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;
- on a confidential basis to a professional adviser, consultant, supplier or other person engaged by any Crown Body (including any benchmarking organisation) for any purpose connected with this contract;
- on a confidential basis for the purpose of the exercise of its rights under this contract;
- on a confidential basis to a proposed successor body of the *Client* in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under this contract,

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the *Client* under this Z clause.

#### **Option Z 14 Security Requirements**

The *Contractor* complies with, and procures the compliance of the Contractor Personnel, with:

- the Security Policy and the Security Management Plan and the *Contractor* shall ensure that the Security Management Plan produced by the *Contractor* fully complies with the Security Policy;
- Contract Schedule J (Security Provisions).

#### **Option Z 16**

##### **Tax Compliance**

Insert new clauses:

29.18 The *Contractor* represents and warrants that as at the Contract Date, it has notified the *Client* in writing of any Occasions of Tax Non-Compliance or any litigation that it is involved in that is in connection with any Occasions of Tax Non-Compliance.

29.19 If, at any point prior to the end of the *defects correction period*, an Occasion of Tax Non-Compliance occurs, the *Contractor* shall:

- notify the *Client* in writing of such fact within 5 days of its occurrence; and
- promptly provide to the *Client*:
  - details of the steps which the *Contractor* is taking to address the Occasions of Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and
  - such other information in relation to the Occasion of Tax Non-Compliance as the *Client* may reasonably require.

**Z19 Project Bank Accounts** Add new clause Z19

Z19.1: Delete the words 'and the *Contractor*' in clause Y1.1(3), line 2.

Z19.2: Delete word '*Contractor*' and **insert** word '*Client*' in clause Y1.2, line 1.

Z19.3: Delete the word '*Contractor*' and **insert** word '*Client*' in clause Y1.3, line 1.

Z19.4: Delete clause Y1.4.

Z19.5: In Y1.8, delete last word "and" of the first bullet point and all of the second bullet point.

**Option Z 22**

**Fair payment**

Insert a new clause:

57.1 The *Contractor* assesses the amount due to a Subcontractor without taking into account the amount certified by the *Project Manager*.

57.2 The *Contractor* includes in the contract with each Subcontractor

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

## **Z26: Building Information Modelling (BIM)**

21A.1 A BIM Protocol applies/does not apply [delete as appropriate]

21A.2 When a BIM Protocol applies it is detailed in the Employer's Information Requirements

21A.3 When the CIC Building Information Modelling Protocol applies clauses 21.A.4 to 21.A.6 shall apply

21A.4 In this clause, the Protocol is the CIC Building Information Modelling Protocol, first edition 2013. Terms used in this clause are those defined in the Protocol.

21A.5 Clauses 1, 2, 5, 6, 7 of the Protocol are *additional conditions of contract*. Clauses 3 and 4 and Appendices 1 and 2 of the Protocol are Scope.

21A.6: The following are compensation events:

- The *Contractor* encounters an event which is outside its reasonable control and which prevents it from carrying out the work specified in clause 4.1.2 of the Protocol.
- The *Client* revokes a licence granted under clause 6.6 of the Protocol.

### **Option Z 42**

#### **The Housing Grants, Construction and Regeneration Act 1996**

Add an additional clause Y2.6

Y2.6

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 works carried out in Northern Ireland]

### **Option Z 44**

#### **Intellectual Property Rights**

Delete clause 22 and insert the following clause

In this clause 22 only:

**"Intellectual Property Rights"** means any and all patents, trademarks, service marks, copyright, moral rights, rights in a design, know-how, Confidential Information and all or any other intellectual or industrial property rights whether or not registered or capable of registration and whether subsisting in the United Kingdom or any other part of the world together with all or any goodwill relating or attached thereto;

**"Confidential Information"** means any information designated as such by the Party disclosing that



information; and

**“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 *Contractor* in relation to this contract.

22.1 The Intellectual Property Rights in all Documents prepared by or on behalf of the *Contractor* in relation to this contract and the work executed from them remains the property of the *Contractor*. The *Contractor* hereby grants to the *Client* an irrevocable, royalty free, non-exclusive licence to use and reproduce the Documents for any and all purposes connected with the Affected Property. Such licence entitles the *Client* to grant sub-licences to third parties in the same terms as this licence provided always that the *Contractor* shall not be liable to any licensee for any use of the Documents or the Intellectual Property Rights in the Documents for purposes other than those for which the same were originally prepared by or on behalf of the *Contractor*.

22.2 The *Client* may assign novate or otherwise transfer its rights and obligations under the licence granted pursuant to 22.1 to a Crown Body or to anybody (including any private sector body) which performs or carries on any functions and/or activities that previously had been performed and/or carried on by the *Client*.

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

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

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

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

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

22.8 After the termination or conclusion of the *Contractor's* employment hereunder, the *Contractor* supplies the *Project Manager* with copies and/or computer discs of such of the Documents as the

*Project Manager* may from time to time request and the *Client* pays the *Contractor's* reasonable costs for producing such copies or discs.

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

#### **Option Z 46**

##### **MoD DEFCON Requirements**

Insert a new clause:

19B

This clause is to incorporate MoD special terms and conditions in the form of DEFCONs and DEFORMs as detailed in Contract Schedule M.

#### **Z 47**

##### **Small and Medium Sized Enterprises (SMEs)**

Insert new clauses:

26.40

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

26.41

The *Contractor* is required to report to the *Client* in its regular contract management monthly reporting cycle the numbers of SMEs engaged as Subcontractors and the value of the Defined Cost of the *works* that has been undertaken by SMEs.

26.42

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

26.43

The *Contractor* is to ensure that the terms and conditions used to engage Subcontractors are no less favourable than those of this contract. A reason for the *Project Manager* not accepting subcontract conditions proposed by the *Contractor* is that they are unduly disadvantageous to the Subcontractor.

## Option Z 48

### Apprenticeships

Insert new clauses:

26.44

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

26.45

The *Contractor* takes all reasonable steps to ensure that no less than the percentage of its employees stated in the Contract Data (the "Apprenticeship Percentage") are on formal apprenticeship programmes or that a similar proportion of hours worked in delivering the *works*, (which may include support staff and Subcontractors) are provided by employees on formal apprenticeship programmes.

26.46

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

26.47

The *Contractor* provides any further skills training opportunities that are appropriate for its employees engaged in carrying out the *works*.

26.48

The *Contractor* 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 *Project Manager*:

- the number of people during the reporting period employed on the contract, including support staff and Subcontractors;
- the number of apprentices and number of new starts on apprenticeships directly initiated through the procurement process;
- the percentage of all employees taking part in an apprenticeship programme;

- if applicable, an explanation from the *Contractor* as to why it is not managing to meet the specified percentage target;
- actions being taken to improve the take up of apprenticeships;
- other training/skills development being undertaken by employees 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.

#### **Z100**

Insert new clause Z100 as follows:

##### **Z100 GDPR**

The *Client* and the *Contractor* shall comply with the provisions of schedule [Guidance: insert schedule ref here]

#### **Z101**

Insert new clause Z101 as follows:

##### **Z101 Cyber Essentials**

The *Client* and the *Contractor* shall comply with the provisions of schedule [Guidance: insert schedule ref here]

**SCHEDULE**[Guidance: insert schedule ref here]

**GDPR**

The following definitions shall apply to this Schedule [Guidance: insert schedule ref here]

**Party** : a Party to this Agreement

**Agreement** : this contract;

**Law** : means any law, 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, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply;

**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, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 subject to Royal Assent to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;

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

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

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)

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

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

Protective Measures : appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule [x] (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 *Client* is the Controller and the Contractor is the Processor unless otherwise specified in Schedule

[X]. The only processing that the Processor is authorised to do is listed in Schedule [X] 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 *works*;
- (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 [ X ], unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;
- (b) ensure that it has in place Protective Measures, are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:

- (i) nature of the data to be protected;
  - (ii) harm that might result from a Data Loss Event;
  - (iii) state of technological development; and
  - (iv) cost of implementing any measures;
- (c) ensure that :
- (i) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule X);
  - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
    - (A) are aware of and comply with the Processor's duties under this clause;
    - (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
    - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and
    - (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
  - (d) not transfer Personal Data outside of the EU 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 (whether in accordance with GDPR Article 46 or LED Article 37) 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 [X] 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 [X] 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 [X] 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: [Insert Contact details]
2. The contact details of the Processor's Data Protection Officer are: [Insert Contact 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	<p>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor in accordance with Clause 1.1.</p> <p>[Guidance: You may need to vary this section where (in the rare case) the Customer and Contractor have a different relationship. For example where the Parties are Joint Controller of some Personal Data:</p> <p>"Notwithstanding Clause 1.1 the Parties acknowledge that they are also Joint Controllers for the purposes of the Data Protection Legislation in respect of:</p> <p style="padding-left: 40px;">[Insert the scope of Personal Data which the purposes and means of the processing is determined by the both Parties]</p> <p>In respect of Personal Data under Joint Control, Clause 1.1-1.15 will not apply and the Parties agree to put in place a Joint Controller Agreement as outlined in Schedule Y instead."</p>
Subject matter of the processing	<p>[This should be a high level, short description of what the processing is about i.e. its subject matter of the contract.</p> <p>Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public. ]</p>
Duration of the processing	[Clearly set out the duration of the processing including dates]
Nature and purposes of the processing	<p>[Please be as specific as possible, but make sure that you cover all intended purposes.</p> <p>The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</p>

	The purpose might include: employment processing, statutory obligation, recruitment assessment etc]
Type of Personal Data being Processed	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]
Categories of Data Subject	[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]
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	[Describe how long the data will be retained for, how it be returned or destroyed]

## SCHEDULE J

### 1. CONTRACT SCHEDULE J - SECURITY PROVISIONS

#### 1.1 Definitions

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

<b>"Affiliates"</b>	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;
<b>"Breach of Security"</b>	<p>in accordance with the Security Requirements and the Security Policy, the occurrence of:</p> <ul style="list-style-type: none"><li>(a) any unauthorised access to or use of the works the <i>Client</i> Premises, the Sites, the Contractor System and/or any ICT, information or data (including the Confidential Information and the <i>Client</i> Data) used by the <i>Client</i> and/or the <i>Contractor</i> in connection with this contract; and/or</li><li>(b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the <i>Client</i> Data), including any copies of such information or data, used by the <i>Client</i> and/or the <i>Contractor</i> in connection with this contract.</li></ul>
<b>"Clearance"</b>	means national security clearance and employment checks undertaken by and/or obtained from the Defence Vetting Agency;
<b>"Contractor Equipment"</b>	the hardware, computer and telecoms devices and equipment supplied by the <i>Contractor</i> or its Subcontractors (but not hired, leased or loaned from the <i>Client</i> ) for the carrying out of the <i>works</i> ;
<b>"Contractor Software"</b>	software which is proprietary to the <i>Contractor</i> , including software which is or will be used by the <i>Contractor</i> for the purposes of carrying out of the <i>works</i> ;
<b>"Contractor System"</b>	the information and communications technology system used by the <i>Contractor</i> in carrying out of the <i>works</i> including the Software, the <i>Contractor</i> Equipment and related cabling (but excluding the <i>Client</i> System);
<b>"Control"</b>	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

### Standard 'boilerplate' amendments

be interpreted accordingly;

<b>"Default"</b>	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 contractors 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;
<b>"Dispute Resolution Procedure"</b>	the dispute resolution procedure set out in this contract (if any) or as agreed between the parties;
<b>"Client Premises"</b>	means premises owned, controlled or occupied by the <i>Client</i> or its Affiliates which are made available for use by the <i>Contractor</i> or its Subcontractors for carrying out of the <i>works</i> (or any of them) on the terms set out in this contract or any separate agreement or licence;
<b>"Client System"</b>	the <i>Client's</i> computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the <i>Client</i> or the <i>Contractor</i> in connection with this contract which is owned by or licensed to the <i>Client</i> by a third party and which interfaces with the <i>Contractor</i> System or which is necessary for the <i>Client</i> to receive the <i>works</i> ;
<b>"Environmental Information Regulations"</b>	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;
<b>"FOIA"</b>	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;
<b>"Good Industry Practice"</b>	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;
<b>"ICT"</b>	information and communications technology;
<b>"ICT Environment"</b>	the <i>Client</i> System and the <i>Contractor</i> System;
<b>"Impact Assessment"</b>	an assessment of a Change Request;
<b>"Information"</b>	has the meaning given under section 84 of the Freedom of Information Act 2000;
<b>"Information Assets"</b>	the register of information assets to be created and maintained by

*Standard 'boilerplate' amendments*

<b>"Register"</b>	the <i>Contractor</i> throughout the carrying out of the <i>works</i> as described in the contract (if any) or as otherwise agreed between the parties;
<b>"ISMS"</b>	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 <i>works</i> ;
<b>"Know-How"</b>	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the <i>works</i> but excluding know how already in the <i>Contractor's</i> or the <i>Client's</i> possession before this contract;
<b>"List x"</b>	means, in relation to a Subcontractor, one who has been placed on List x in accordance with Ministry of Defence guidelines and procedures, due to that Sub contractor undertaking work on its premises marked as CONFIDENTIAL or above;
<b>"Malicious Software"</b>	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;
<b>"Process"</b>	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;
<b>"Protectively Marked"</b>	shall have the meaning as set out in the Security Policy Framework.
<b>"Regulatory Bodies"</b>	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 <i>Client</i> and "Regulatory Body" shall be construed accordingly;
<b>"Request for Information"</b>	a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations;
<b>"Security Management Plan"</b>	the <i>Contractor's</i> 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);
<b>"Security Policy Framework"</b>	means the Cabinet Office Security Policy Framework (available from the Cabinet Office Security Policy Division);

## Standard 'boilerplate' amendments

<b>"Security Requirements"</b>	means the requirements in the contract relating to security of the carrying out of the <i>works</i> (if any) or such other requirements as the <i>Client</i> may notify to the <i>Contractor</i> from time to time
<b>"Security Tests"</b>	shall have the meaning set out in paragraph 2.4.1 of Part 2 of this Contract Schedule J (Security Management Plan);
<b>"Sites"</b>	any premises at which the <i>works</i> are carried out or from which the <i>Contractor</i> manages, organises or otherwise directs the provision or the carrying out of the <i>works</i> or where any part of the <i>Contractor</i> System is situated or where any physical interface with the <i>Client</i> System takes place;
<b>"Software"</b>	Specially Written Software, <i>Contractor</i> Software and Third Party Software;
<b>"Specially Written Software"</b>	any software created by the <i>Contractor</i> (or by a third party on behalf of the <i>Contractor</i> ) specifically for the purposes of this contract;
<b>"Staff Vetting Procedures"</b>	the <i>Client's</i> 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;
<b>"Statement of Applicability"</b>	shall have the meaning set out in ISO/IEC 27001 and as agreed by the parties during the procurement phase;
<b>"Standards"</b>	the British or international standards,[ <i>Client's</i> 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;
<b>"Third Party Software"</b>	software which is proprietary to any third party other than an Affiliate of the <i>Contractor</i> which is or will be used by the <i>Contractor</i> for the purposes of carrying out of the <i>works</i> ; and

## 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 *works*;
- 1.2.1.2 wider aspects of security relating to carrying out of the *works*;

*Standard 'boilerplate' amendments*

- 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 *Contractor* acknowledges that the *Client* places great emphasis on the confidentiality, integrity and availability of information and consequently on the security provided by the ISMS.
- 1.3.2 The *Contractor* 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 *Client'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 *Contractor* gives an early warning to the *Project Manager* of such inconsistency immediately upon becoming aware of the same, and the *Project Manager* shall, as soon as practicable, advise the *Contractor* which provision the *Contractor* shall be required to comply with.



*Standard 'boilerplate' amendments*

1.4 ISMS and Security Management Plan

1.4.1 Introduction:

- 1.4.1.1 The *Contractor* shall develop, implement, operate, maintain and continuously improve and maintain an ISMS which will, without prejudice to paragraph 1.3.2, be approved, by the *Project Manager*, 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.
- 1.4.1.2 The *Contractor* shall develop and maintain a Security Management Plan in accordance with this Schedule to apply during the carrying out of the *works*.
- 1.4.1.3 The *Contractor* shall comply with its obligations set out in the Security Management Plan.
- 1.4.1.4 Both the ISMS and the Security Management Plan shall, unless otherwise specified by the *Client*, aim to protect all aspects of the *works* and all processes associated with carrying out of the *works*, including the Affected Property, the *Contractor* System and any ICT, information and data (including the *Client* Confidential Information and the *Client* Data) to the extent used by the *Client* or the *Contractor* 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 *Contractor* will prepare and deliver to the *Project Manager* for approval 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 approved by the *Project Manager* 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 approved by the *Project Manager* the *Contractor* shall amend it within 10 Working Days or such other period as the parties may agree in writing of a notice of non-approval from the *Project Manager* and re-submit to the *Project Manager* for approval. The parties will use all reasonable endeavours to ensure that the approval 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 *Project Manager*. If the *Project Manager* does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. No

### Standard 'boilerplate' amendments

approval to be given by the *Project Manager* pursuant to this paragraph 1.4.2.2 of this schedule may be unreasonably withheld or delayed. However any failure to approve 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 *Contractor* in relation to all aspects of the *works* and all processes associated with carrying out of the *works* and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the *works* 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 *Contractor's* ISMS at the date notified by the *Project Manager* to the *Contractor* for the *Contractor* 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 *Contractor* and the *Client* engaged in the *works* and shall only reference documents which are in the possession of the *Client* 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 *Contractor* annually or from time to time to reflect:
  - (a) emerging changes in Good Industry Practice;
  - (b) any change or proposed change to the *Contractor* System, the *works* and/or associated processes;
  - (c) any new perceived or changed security threats; and
  - (d) any reasonable request by the *Project Manager*.
- 1.4.4.2 The *Contractor* will provide the *Project Manager* 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

### Standard 'boilerplate' amendments

cost to the *Client*. 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 *Project Manager* will approve 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 *Contractor* proposes to make to the ISMS or Security Management Plan (as a result of a *Project Manager's* request or change to the *works* or otherwise) shall be subject to the early warning procedure and shall not be implemented until approved in writing by the *Project Manager*.

#### 1.4.5 Testing

1.4.5.1 The *Contractor* shall conduct tests of the ISMS ("Security Tests") 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 *Project Manager*.

1.4.5.2 The *Project Manager* shall be entitled to witness the conduct of the Security Tests. The *Contractor* shall provide the *Project Manager* with the results of such tests (in a form approved by the *Client* 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 *Client* pursuant to this contract, the *Project Manager* and/or its authorised representatives shall be entitled, at any time and without giving notice to the *Contractor*, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the *Contractor's* compliance with the ISMS and the Security Management Plan. The *Project Manager* may notify the *Contractor* 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 *works*. If such tests adversely affect the *Contractor's* ability to carry out the *works* in accordance with the Scope, the *Contractor* shall be granted relief against any resultant under-performance for the period of the tests.

*Standard 'boilerplate' amendments*

- 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 *Contractor* shall promptly notify the *Project Manager* of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the *Contractor* proposes to make in order to correct such failure or weakness. Subject to the *Project Manager's* approval in accordance with paragraph 1.4.1.1, the *Contractor* shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the *Project Manager* or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan to address a non-compliance with the Security Policy or Security Requirements the change to the ISMS or Security Management Plan shall be at no cost to the *Client*.

1.5 Compliance with ISO/IEC 27001

- 1.5.1 Unless otherwise agreed by the parties, the *Contractor* shall obtain independent certification of the ISMS to ISO/IEC 27001 within 12 months of the Contract Date and shall maintain such certification for the duration of the contract.
- 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 *Contractor* reasonably believes that it is not compliant with ISO/IEC 27001, the *Contractor* shall promptly notify the *Project Manager* of this and the *Client* in its absolute discretion may waive the requirement for certification in respect of the relevant parts.
- 1.5.3 The *Project Manager* 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 *Project Manager's* reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the *Contractor*, then the *Project Manager* shall notify the *Contractor* of the same and give the *Contractor* 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 *Contractor* does not become compliant within the required time then the *Project Manager* 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 *Contractor* is found to be non-compliant with the principles and practices of ISO/IEC 27001 then the *Contractor* 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 *Client* in obtaining such audit.

1.6 Breach of Security

*Standard 'boilerplate' amendments*

- 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 *Contractor* 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 *Project Manager*; and
- 1.6.2.2 as soon as reasonably practicable provide to the *Project Manager* 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**

*[Guidance Note: Append Security Policy]*

**Appendix 2 – Security Management Plan**

*[Guidance Note: Append Security Management Plan]*

**SCHEDULE** [Guidance: insert schedule ref here]

**CYBER ESSENTIALS**

**CYBER ESSENTIALS SCHEME**

**1. DEFINITIONS**

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

<b>"Cyber Essentials Scheme"</b>	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: <a href="https://www.gov.uk/government/publications/cyber-essentials-scheme-overview">https://www.gov.uk/government/publications/cyber-essentials-scheme-overview</a> ;
<b>"Cyber Essentials Basic Certificate"</b>	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;
<b>"Cyber Essentials Certificate"</b>	Cyber Essentials Basic Certificate, the Cyber Essentials Plus Certificate or the Cyber Essential Scheme certificate equivalent to be provided by the <i>Contractor</i> as set out in the Framework Data Sheet;
<b>"Cyber Essential Scheme Data"</b>	sensitive and personal information and other relevant information as referred to in the Cyber Essentials Scheme; and
<b>"Cyber Essentials Plus Certificate"</b>	the certification awarded on the basis of external testing by an independent certification body of the <i>Contractor's</i> 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 *Contractor* provide a Cyber Essentials Certificate prior to the execution of the *works* the *Contractor* shall provide a valid Cyber Essentials Certificate, then on or

prior to the commencement of the *works* the *Contractor* delivers to the *Client* evidence of the same. Where the *Contractor* fails to comply with this paragraph it shall be prohibited from commencing the carrying out of the *works* under any contract until such time as the *Contractor* has evidenced to the *Client* its compliance with this paragraph 2.1.

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

2.3 Where the *Contractor* is due to Process Cyber Essentials Scheme Data after the commencement of the *works* but before completion of the *works* the *Contractor* delivers to the *Client* evidence of:

2.3.1 a valid and current Cyber Essentials Certificate before the *Contractor* 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 *Contractor* under paragraph 2.1.

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

2.5 The *Contractor* ensures that all sub-contracts with Sub-Contractors who Process Cyber Essentials Data contain provisions no less onerous on the Sub-Contractors than those imposed on the *Contractor* 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

**SCHEDULE OF AMENDMENTS TO JCT DESIGN AND BUILD CONTRACT 2016 EDITION/JCT STANDARD BUILDING CONTRACT WITH QUANTITIES 2016 EDITION/WITHOUT QUANTITIES EDITION/INTERMEDIATE BUILDING CONTRACT WITH CONTRACTOR'S DESIGN 2016 DESIGN, INTERMEDIATE BUILDING CONTRACT 2016 EDITION**

**Interpretation Table**

Due to the different clause numbering in the different versions of the JCT, the terms of the interpretation table below shall apply with clause references and clause cross referencing to be read according to the table.

<b>Schedule Of Amendments Reference Below</b>	<b>Design And Build 2016 Edition</b>	<b>Standard Building Contract With Quantities 2016 Edition</b>	<b>Standard Building Contract Without Quantities 2016 Edition</b>	<b>Intermediate Building Contract With Contractor's Design 2016 Design</b>	<b>Intermediate Building Contract 2016 Edition</b>
1.13 to 1.20	1.12 to 1.19	No change	No change	No change	No change
2.1A to 2.1C	2.1.5 to 2.1.7	No change	No change	No change	No change
2.41	2.38	No change	No change	2.33	2.1.D (insertion- see below for further details)
3.9	3.4	No change	No change	3.6	3.6



3.9A and 3.9B	3.4A and 3.4B	No change	No change	3.6A and 3.6B	3.6A and 3.6B
---------------	------------------	-----------	-----------	------------------	------------------

In addition, for the JCT Design and Build Contract 2016 Edition, all references to “Architect/Contract Administrator” below shall be read as “Employer’s Agent” and all references to “Variation” shall be read as “Change”

Unless specified, all clauses below apply to all forms of contract.

**Insert** new article:

**"Article 10: Schedule of Amendments**

The Contract is modified by the Schedule of Amendments (which has been initialled on behalf of both parties) and is to be read and construed accordingly."

*[Preparation Note: Unless an electronic version of the JCT contract is being used AND this new Article has been inserted in the text of it as an amendment, this new Article MUST be written, in manuscript, at the end of the Articles on the face of each original standard form JCT contract to be executed by the parties.]*

**Clause 1.1. Definitions**

**Insert** the following new definitions:

"Commercially Sensitive Information: the information agreed between the parties (if any) comprising the information of a commercially sensitive nature relating to the Contractor, the charges for the Works, its IPR or its business or which the Contractor has indicated to the Employer that, if disclosed by the Employer, would cause the Contractor significant commercial disadvantage or material financial loss;

Confidential Information: the Employer's Confidential Information and/or the Contractor's Confidential Information;

Contracting Body: any Contracting Body as defined in Regulation 5(2) of the Public Contracts (Works, Service and Supply) (Amendment) Regulations 2000 other than the Employer.

Contractor's Confidential Information: any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and contractors of the Contractor, 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;

Crown Body: any department, office or agency of the Crown

Data Controller: has the meaning given to it in the Data Protection Act 2018

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.

Employer Confidential Information: 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

Employer Data:

- 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 Contractor by or on behalf of the Employer; or
  - which the Contractor 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 Contractor.

Environmental Information Regulations: the Environmental Information Regulations 2004 and any guidance and/or codes of practice issued by the Information Commissioner 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 in relation to such legislation;

General Anti-Abuse Rule:

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

Halifax Abuse Principle: the principle explained in the CJEU Case C-255/02 Halifax and others

Intellectual Property Rights or "IPRs":

(a) 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;

(b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and

(c) all other rights having equivalent or similar effect in any country or jurisdiction;

Law: 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 Contractor is bound to comply;

Occasion of Tax Non-Compliance:

- where any tax return of the Contractor 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 Contractor 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;
- The failure of an avoidance scheme which the Contractor was involved in, and which was, or should have been, notified to a Relevant Tax Authority under DOTAS or any equivalent or similar regime; and/or

where any tax return of the Contractor 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.

Personal Data: the meaning given to it in the Data Protection Act 2018

Prohibited Act:

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.

**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 Information Regulations

**Relevant Requirements:** 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

**Relevant Tax Authority:** HM Revenue & Customs, or, if applicable, a tax authority in the jurisdiction in which the Contractor is established.

**Security Policy:** the Employer's security policy attached as Appendix 1 to Schedule [Guidance: insert schedule ref here] (Security Policy) as may be updated from time to time"

#### **1.6 Contracts (Rights of Third Parties) Act 1999**

1.6 In clause 1.6 After "clauses 7A and/or 7B" **insert** "and the express rights of any person under any collateral warranty granted under the provisions of this Contract," [All contracts except the Intermediate Forms of contract]

1.6 In clause 1.6 **delete** "Notwithstanding any other provision of this Contract," and **insert** "Subject to the express rights of any person under any collateral warranty granted under the provisions of this Contract," [Intermediate Forms of contract]

**Insert** new clauses 1.13 to 1.20 as follows:

#### **MoD DEFCON Requirements**

1.13 The MoD special terms and conditions in the form of DEFCONs and DEFORMs shall be incorporated into this Contract as detailed in Contract Schedule [Guidance: insert schedule ref here]

## **Freedom of information**

1.14.1 The Contractor acknowledges that unless the Architect/Contract Administrator has notified the Contractor 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, FOIA and the Environmental Information Regulations. The Contractor shall co-operate with and assist the Employer so as to enable the Employer to comply with its information disclosure obligations.

1.14.2 The Contractor shall:

1.14.2.1 transfer to the Architect/Contract Administrator 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;

1.14.2.2 provide the Architect/Contract Administrator with a copy of all Information in its possession, or power in the form that the Architect/Contract Administrator shall require within five Working Days (or such other period as the Architect/Contract Administrator may specify) of the Architect/Contract Administrator's request;

1.14.2.3 provide all necessary assistance as reasonably requested by the Architect/Contract Administrator 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

1.14.2.4 procures that its sub-contractors do likewise.

1.14.3 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.

1.14.4 The Contractor shall not respond directly to a Request for Information unless authorised to do so by the Architect/Contract Administrator.

1.14.5 The Contractor 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 Contractor or despite the Contractor having expressed negative views when consulted.

1.14.6 The Contractor shall ensure that all Information is retained for disclosure for twelve years where this Contract is executed as a deed or six years where this Contract is executed under hand and shall permit the Architect/Contract Administrator to inspect such records as and when reasonably requested from time to time."

## **1.15 Tax Compliance**

1.15.1 The Contractor represents and warrants that as at the date of this Contract, 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.

1.15.2 If, at any point prior to the end of the Rectification Period, an Occasion of Tax Non-Compliance occurs, the Contractor shall:

1.15.2.1 notify the Employer in writing of such fact within 5 days of its occurrence; and

1.15.2.2 promptly provide to the Employer:

1.15.2.2.1 details of the steps which the Contractor 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

1.15.2.2.2 such other information in relation to the Occasion of Tax Non-Compliance as the Employer may reasonably require.

#### **1.16 GDPR**

The Employer and the Contractor shall comply with the provisions of schedule [Guidance: insert schedule ref here]

#### **1.17 Confidentiality and Information Sharing**

1.17.1 Except to the extent set out in this clause or where disclosure is expressly permitted elsewhere in this Contract, each party shall:

1.17.1.1 treat the other party's Confidential Information as confidential and safeguard it accordingly; and

1.17.1.2 not disclose the other party's Confidential Information to any other person without the owner's prior written consent.

1.17.1.3 immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information

1.17.1.4 notify the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010

1.17.2 The clause above shall not apply to the extent that:

1.17.2.1 such disclosure is a requirement of the law of the contract placed upon the party making the disclosure, including any requirements for disclosure under the FOIA or the Environmental Information Regulations pursuant to clause 1.14 (Freedom of Information);

1.17.2.2 such information was in the possession of the party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;

1.17.2.3 such information was obtained from a third party without obligation of confidentiality;

1.17.2.4 such information was already in the public domain at the time of disclosure otherwise than by a breach of this Contract; or

1.17.2.5 it is independently developed without access to the other party's Confidential Information.

1.17.3 The Contractor may only disclose the Employer's Confidential Information to Contractor's Persons who are directly involved in the carrying out of the Works and who need to know the information, and shall ensure that such Contractor's Persons are aware of and shall comply with these obligations as to confidentiality.

1.17.4 The Contractor shall not, and shall procure that the Contractor's Persons do not, use any of the Employer's Confidential Information received otherwise than for the purposes of this Contract.

1.17.5 The Contractor may only disclose the Employer's Confidential Information to Contractor's Persons who need to know the information, and shall ensure that such Contractor's Persons 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 Contractor's Persons causes or contributes (or could cause or contribute) to the Contractor breaching its obligations as to confidentiality under or in connection with this Contract, the Contractor 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 Contractor Personnel, the Contractor 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 Contractor is taking appropriate steps to comply with this clause, including copies of any written communications to and/or from Contractor's Persons, and any minutes of meetings and any other records which provide an audit trail of any discussions or exchanges with Contractor's Persons in connection with obligations as to confidentiality.

1.17.6 At the written request of the Employer, the Contractor shall procure that those members of the Contractor's Persons identified in the Employer's notice signs a confidentiality undertaking prior to commencing any work in accordance with this Contract.

1.17.7 Nothing in this Contract shall prevent the Employer from disclosing the Contractor's Confidential Information:

1.17.7.1 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 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;

1.17.7.2 to any consultant, contractor or other person engaged by the Employer or any person conducting an Office of Government Commerce gateway review;

1.17.7.3 for the purpose of the examination and certification of the Employer's accounts; or

1.17.7.4 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.

and for the purposes of the foregoing, disclosure of the Contractor'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 1.17.

1.17.8 The Employer shall use all reasonable endeavours to ensure that any government department, Contracting Body, employee, third party or sub-contractor to whom the Contractor's Confidential Information is disclosed pursuant to the above clause is made aware of the Employer's obligations of confidentiality.

1.17.9 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

1.17.10 The Employer may disclose the Confidential Information of the Contractor:



- 1.17.10.1 on a confidential basis to any Crown Body for any proper purpose of the Employer or the relevant Crown Body;
- 1.17.10.2 to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;
- 1.17.10.3 to the extent that the Employer (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;
- 1.17.10.4 on a confidential basis to a professional adviser, consultant, supplier or other person engaged by any Crown Body (including any benchmarking organisation) for any purpose connected with this Contract;
- 1.17.10.5 on a confidential basis for the purpose of the exercise of its rights under this Contract;
- 1.17.10.6 on a confidential basis 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, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Employer under this clause.

#### **1.18 Prevention of Fraud and Bribery**

- 1.18.1 The Contractor represents and warrants that neither it, nor to the best of its knowledge any of its employees, have at any time prior to the date of this Contract:
  - 1.18.1.1 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
  - 1.18.1.2 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.
- 1.18.2 During the carrying out of the Works the Contractor shall not:
  - 1.18.2.1 commit a Prohibited Act; and/or
  - 1.18.2.2 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
- 1.18.3 During the carrying out of the Works the Contractor shall:
  - 1.18.3.1 establish, maintain and enforce, and require that its sub-contractors 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;
  - 1.18.3.2 keep appropriate records of its compliance with this Contract and make such records available to the Employer on request;
  - 1.18.3.3 provide and maintain and where appropriate enforce an anti-bribery policy (which shall be disclosed to the Employer on request) to prevent it and any Contractor's employees or any person acting on the Contractor's behalf from committing a Prohibited Act.
- 1.18.4 The Contractor shall notify the Employer immediately in writing if it becomes aware of any breach of clause 1.18.1, or has reason to believe that it has or any of its employees or sub-contractors have:



1.18.4.1 been subject to an investigation or prosecution which relates to an alleged Prohibited Act;

1.18.4.2 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; and/or

1.18.4.3 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.

1.18.5 If the Contractor shall make a notification to the Employer pursuant to clause 1.18.4, the Contractor shall respond promptly to the Employer's enquiries, co-operate with any investigation, and allow the Employer to audit any books, records and/or any other relevant documentation in accordance with this Contract.

1.18.6 If the Contractor breaches Clause 1.18.3, the Employer may by notice require the Contractor to remove from carrying out the Works any Contractor's Person whose acts or omissions have caused the Contractor's breach.

### **1.19 Security requirements**

The Contractor shall comply with, and procure the compliance of the Contractor's Persons, with:

1.19.1 the Security Policy and the Security Management Plan and the Contractor shall ensure that the Security Management Plan produced by the Contractor fully complies with the Security Policy;

1.19.2 Contract Schedule [Guidance: insert schedule ref here] (Security Provisions).

### **1.20 Cyber Essentials**

The Employer and the Contractor shall comply with the provisions of schedule [Guidance: insert schedule ref here]

## **2.1 General Obligations**

**Insert** new clauses 2.1A to 2.1C as follows:

### **"2.1A Admittance to the site**

2.1.A.1 The Contractor shall submit details of people who are to be employed by it and its sub-contractors in connection with the Works to the Architect/Contract Administrator. The details shall include a list of names and addresses, the capabilities in which they are employed, and other information required by the Architect/Contract Administrator.

2.1.A.2 The Architect/Contract Administrator may instruct the Contractor to take measures to prevent unauthorised persons being admitted to site. The instruction shall be valued as a Variation if the measures are additional to those required by the Employer's Requirements.

2.1.A.3 Contractor's Persons are to carry an Employer's pass and comply with all conduct requirements from the Employer whilst they are on the parts of the site identified in the Employer's Requirements.

2.1.A.4 The Contractor shall submit to the Architect/Contract Administrator for acceptance a list of the names of the people for whom passes are required. On acceptance, the Architect/Contract Administrator shall issue the passes to the Contractor. Each pass shall be returned to the Architect/Contract Administrator when the employee no longer requires access to that part of the site or after the Architect/Contract Administrator has given notice that the employee is not to be admitted to the site.

2.1.A.5 The Contractor shall not take photographs of the site or of work carried out in connection with the Works unless it has obtained the acceptance of the Architect/Contract Administrator.

2.1.A.6 The Contractor shall take the measures needed to prevent any Contractor's Persons taking, publishing or otherwise circulating such photographs.

#### **2.1.B Legislation and Official secrets**

2.1.B.1 The Contractor shall comply with the Law in the carrying out of the Works.

2.1.B.2 The Official Secrets Acts 1911 to 1989 and, where appropriate, the provisions of section 11 of the Atomic Energy Act 1946 apply to this Contract.

2.1.B.3 The Contractor shall notify its employees and its sub-contractors of their duties under these Acts.

#### **2.1.C Building Information Modelling**

2.1.C.1 A BIM Protocol applies/does not apply [delete as appropriate]

2.1.C.2 When a BIM Protocol applies it is detailed in the Employer's Information Requirements

2.1.C.3 When the CIC Building Information Modelling Protocol applies clauses 2.1.C.4 to 2.1.C.6.2 shall apply

2.1.C.4 In this clause, the Protocol is the CIC Building Information Modelling Protocol, first edition 2013. Terms used in this clause are those defined in the Protocol.

2.1.C.5 Clauses 1, 2, 5, 6, 7 of the Protocol shall form part of this Contract. Clauses 3 and 4 and Appendices 1 and 2 of the Protocol are deemed to be part of the Client's Requirements.

2.1.C.6: The following shall be deemed to be a Change:

2.1.C.6.1 If the Constructor encounters an event which is outside his reasonable control and which prevents him from carrying out the work specified in clause 4.1.2 of the Protocol.

2.1.C.6.2 If the Client revokes a licence granted under clause 6.6 of the Protocol.

#### **2.41 Copyright and use**

**Delete** clause 2.41 and **insert** new clause 2.41 [all except Intermediate Form of Contract 2016 (no design)] **Insert** new clause 2.1D [Intermediate Form of Contract 2016 (no design)]

"In this clause 2.41 only:

**"Intellectual Property Rights"** means any and all patents, trademarks, service marks, copyright, moral rights, rights in a design, know-how, Confidential Information and all or any other intellectual or industrial property rights whether or not registered or capable of registration and whether subsisting

in the United Kingdom or any other part of the world together with all or any goodwill relating or attached thereto;

**“Confidential Information”** means any information designated as such by the Party disclosing that information; and

**“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 Contractor in relation to this Contract.

2.41.1 The Intellectual Property Rights in all Documents prepared by or on behalf of the Contractor in relation to this Contract and the work executed from them remains the property of the Contractor. The Contractor 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 Site. Such licence entitles the Employer to grant sub-licences to third parties in the same terms as this licence provided always that the Contractor shall not be liable to any licensee for any use of the Documents or the Intellectual Property Rights in the Documents for purposes other than those for which the same were originally prepared by or on behalf of the Contractor.

2.41.2 The Employer may assign, novate or otherwise transfer its rights and obligations under the licence granted pursuant to clause 2.41.2 to a Crown Body or to anybody (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Employer.

2.41.3 In the event that the Contractor does not own the copyright or any Intellectual Property Rights in any Document the Contractor shall use 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 Contractor is unable to procure the right to grant to the Employer in accordance with the foregoing the Contractor shall procure that the third party grants a direct licence to the Employer on industry acceptable terms.

2.41.4 The Contractor 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.

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

2.41.6 The Contractor warrants to the Employer that he 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.

2.41.7 The Contractor shall supply copies of the Documents to the Architect/Contract Administrator 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 works.

2.41.8 After the termination or conclusion of the Contractor's employment hereunder, the Contractor shall supply the Architect/Contract Administrator with copies and/or computer discs of such of the Documents as the Architect/Contract Administrator may from time to time request and the Employer shall pay the Contractor's reasonable costs for producing such copies or discs.

2.41.9 In carrying out the Works the Contractor shall not infringe any Intellectual Property Rights of any third party. The Contractor shall indemnify the Employer against claims, proceedings, compensation and costs arising from an infringement or alleged infringement of the Intellectual Property Rights of any third party. "

### **3.9 Conditions of sub-contracting**

3.9.2.6 to 3.9.2.9 Insert new subclauses 3.9.2.6 to 3.9.2.9 as follows:

"3.9.2.6 a period for payment of the amount due to the sub-contractor not greater than 5 days after the final date for payment in this Contract. The amount due shall, but shall not be limited to, payment for work which the sub-contractor has completed from the previous application date up to the current application date in this Contract;

3.9.2.7 a provision requiring the sub-contractor 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

3.9.2.8 a provision requiring the sub-contractor to assess the amount due to a subsubcontractor without taking into account the amount paid by the Contractor.

3.9.2.9 terms and conditions that are no less favourable than those of this Contract. The Employer shall be entitled to reject sub-contract conditions proposed by the Contractor that are unduly disadvantageous to the sub-contractor"

#### **3.9A Insert new clause 3.9A**

"3.9A.1 The Contractor shall take all reasonable steps to engage SMEs as sub-contractors and to seek to ensure that no less than the percentage of the sub-contractors stated in the Employer's Requirements (the "SME Percentage") are SMEs or that a similar proportion of the Contract Sum is undertaken by SMEs.

3.9A.2 The Contractor shall report to the Employer on a monthly basis the numbers of SMEs engaged as sub-contractors and the value of the Contract Sum that has been undertaken by SMEs.

3.9A.3 Where available, the Contractor shall tender its sub-contracts using the same online electronic portal as was provided by the Employer for the purposes of tendering this Contract.

#### **3.9B Insert new clause 3.9B as follows:**

##### **"3.9B Apprenticeships**

3.9B.1 The Contractor shall take all reasonable steps to employ apprentices, and report to the Employer the numbers of apprentices employed and the wider skills training provided, during the carrying out of the Works.

3.9B.2 The Contractor shall take all reasonable steps to ensure that no less than the percentage of its employees stated in the Employer's Requirements (the "Apprenticeship Percentage") are on formal apprenticeship programmes or that a similar proportion of hours worked in carrying out the Works, (which may include support staff and sub-contractors) are provided by employees on formal apprenticeship programmes.

3.9B.3 The Contractor shall make available to its employees and sub-contractors working on the Contract, information about the Government's Apprenticeship programme and wider skills opportunities.

3.9B.4 The Contractor shall provide any further skills training opportunities that are appropriate for its employees engaged in carrying out the Works.

3.9B.5 The Contractor shall provide a written report detailing the following measures in its regular contract management monthly reporting cycle and be prepared to discuss apprenticeships at its regular meetings with the Architect/Contract Administrator:

- the number of people during the reporting period employed on the Contract, including support staff and sub-contractors;
- the number of apprentices and number of new starts on apprenticeships directly initiated through the procurement process;
- the percentage of all employees taking part in an apprenticeship programme;
- if applicable, an explanation from the Contractor as to why it is not managing to meet the specified percentage target;
- actions being taken to improve the take up of apprenticeships;
- other training/skills development being undertaken by employees 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."

**Insert** new clause 4A as follows:

#### **"4A Project Bank Account**

The parties shall comply with the provisions of Schedule [Guidance: insert schedule ref here]

**SCHEDULE** [Guidance: insert schedule ref here]

**PROJECT BANK**

**ACCOUNT**

**1. Definitions**

The following definitions shall apply to this Schedule

Authorisation: a document authorising the Project Bank to make payments to the Contractor and Named Suppliers.

Named Suppliers: such Suppliers as are detailed in the Employer's Requirements and such other Suppliers who have signed the Joining Deed.

Project Bank: such bank as the Employer shall inform the Contractor in writing

Project Bank Account: the account used to receive payments from the Employer and to make payments to the Contractor and Named Suppliers

A Suppliers: a person or organisation who has a contract to

- construct or install part of the Works,
- provide a service necessary to provide the Works or
- supply Plant and Materials for the Works.

Trust Deed: an agreement in the form set out in the Contract which contains provisions for administering the Project Bank Account.

Joining Deed: an agreement in the form set out in the Contract under which the Supplier joins the Trust Deed.

**2. Project Bank Account**

2.1 The Employer shall establish the Project Bank Account with the Project Bank within three weeks of the date of this Contract.

2.2 Unless stated otherwise in the Employer's Requirements, the Employer shall pay any charges made and is paid any interest paid by the Project Bank. The charges and interest by the Project Bank are not included in the Contract Sum.

### **3. Named Suppliers**

The Contractor shall include in its contracts with Named Suppliers the arrangements in the contract for the operation of the Project Bank Account and Trust Deed. The Contractor shall inform the Named Suppliers of the details of the Project Bank Account and the arrangements for payment of amounts due under their contracts.

### **4. Payments**

4.1 The Contractor shall submit proposals for adding a Supplier to the Suppliers to the Architect/Contract Administrator for acceptance. A reason for not accepting is that the addition of such Supplier would not comply with the Employer's Requirements. The Employer, the Contractor and the Supplier shall sign the Joining Deed after acceptance

4.2 The Contractor shall show in the application for payment the amounts due to Named Suppliers in accordance with their contracts.

4.3 Within the time set out in the banking arrangements to allow the Project Bank to make payment to the Contractor and Named Suppliers in accordance with the Contract, the Employer shall make payment to the Project Bank Account of the amount which is due to be paid under the Contract

4.4 The Contractor shall prepare the Authorisation, setting out the sums due to Named Suppliers as assessed by the Contractor and to the Contractor for the balance of the payment due under the Contract. After signing the Authorisation, the Contractor shall submit it to the Architect/Contract Administrator no later than four days before the final date for payment. The Employer shall sign the Authorisation and submit it to the Project Bank no later than one day before the final date for payment.

4.5 The Contractor and Named Suppliers shall receive payment from the Project Bank Account of the sums set out in the Authorisation as soon as practicable after the Project Bank Account receives payment.

4.6 Any payment which is due from the Contractor to the Employer shall not be made through the Project Bank Account

## **5. Effect of Payment**

Payments made from the Project Bank Account are treated as payments from the Employer to the Contractor in accordance with the Contract or from the Contractor or Supplier to Named Supplier in accordance with their contracts as applicable. A delay in payment due to a failure of the Contractor to comply with the requirements of this clause is not treated as late payment under the Contract.

## **6. Trust Deed**

The Employer, the Contractor and Named Suppliers shall sign the Trust Deed before the first Interim Valuation Date.

## **7. Termination**

If the Architect/Contract Administrator issues a termination certificate, no further payment is to be made into the Project Bank Account.



## FORM OF TRUST DEED

This agreement is made between the "**Employer**", the "**Contractor**" and the Named Suppliers.

Terms in this deed have the meanings given to them in the contract between \_\_\_\_\_ and \_\_\_\_\_  
for ("**Works**").

### BACKGROUND

The Employer and the Contractor have entered into a contract for the Works.

The Named Suppliers have entered into contracts with the Contractor or a subcontractor in connection with the Works.

The Contractor has established a Project Bank Account to make provision for payment to the Contractor and the Named Suppliers.

### AGREEMENT

The parties to this deed agree that:

1. sums due to the Contractor and Named Suppliers and set out in the Authorisation are held in trust in the Project Bank Account by the Contractor for distribution to the Contractor and Named Suppliers in accordance with the banking arrangements applicable to the Project Bank Account.
2. Further Named Suppliers may be added as parties to this deed with the agreement of the Employer and Contractor. The agreement of the Employer and Contractor is treated as agreement by the Named Suppliers who are parties to this deed.
3. This deed is subject to the law of the contract for the Works.
4. The benefits under this deed may not be assigned.

Executed as a deed, but not delivered until the )  
first date specified on page 1 by )  
: )

Signature .....

Name (block capitals) .....

**Employer**

*Standard 'boilerplate' amendments*

Signature .....

Name (block capitals) .....

**Contractor**

Signature .....

Name (block capitals) .....

**Supplier**

## FORM OF JOINING DEED

-----  
This agreement is made between the **"Employer"**, the **"Contractor"** and  
**("Additional Supplier")**.

Terms in this deed have the meanings given to them in the contract between \_\_\_\_\_ and  
for **("Works")**.

### BACKGROUND

The Employer and the Contractor have entered into a contract for the Works.

The Named Suppliers have entered into contracts with the Contractor or a Subcontractor in  
connection with the Works.

The Contractor has established a Project Bank Account to make provision for payment to the  
Contractor and the Named Suppliers.

The Employer, the Contractor and the Named Suppliers have entered into a deed as set out in  
Annex 1 (**"Trust Deed"**), and have agreed that the Additional Supplier may join that deed.

### AGREEMENT

The parties to this deed agree that:

1. The Additional Supplier becomes a party to the Trust Deed from the date set out below.
2. This deed is subject to the law of the contract for the Works.
3. The benefits under this deed may not be assigned.

Executed as a deed, but not delivered until the )  
first date specified on page 1 by )  
:

Signature \_\_\_\_\_

Name (block capitals) \_\_\_\_\_

**Employer**

Signature

*Standard 'boilerplate' amendments*

Name (block capitals) \_\_\_\_\_  
**Contractor**

Signature \_\_\_\_\_

Name (block capitals) \_\_\_\_\_  
**Additional Supplier**

**SCHEDULE** [Guidance: insert schedule ref here]

**GDPR**

The following definitions shall apply to this Schedule [Guidance: insert schedule ref here]

**Party** : a Party to this Agreement

**Agreement** : this contract;

**Law** : means any law, 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, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply;

**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, the LED and any applicable national implementing Laws as amended from time to time (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;

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 GDPR.

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)

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

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

Protective Measures : appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule [x] (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 Contractor is the Processor unless otherwise specified in Schedule

[X]. The only processing that the Processor is authorised to do is listed in Schedule [X] 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 [ X ], unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;
- (b) ensure that it has in place Protective Measures, are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:
  - (i) nature of the data to be protected;
  - (ii) harm that might result from a Data Loss Event;
  - (iii) state of technological development; and
  - (iv) cost of implementing any measures;
- (c) ensure that :
  - (i) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule X);
  - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

- (A) are aware of and comply with the Processor's duties under this clause;
- (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
- (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and
- (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
- (d) not transfer Personal Data outside of the EU 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 (whether in accordance with GDPR Article 46 or LED Article 37) 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 [X] 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 [X] 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 [X] 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.

5. The contact details of the Controller's Data Protection Officer are: [Insert Contact details]
6. The contact details of the Processor's Data Protection Officer are: [Insert Contact details]
7. The Processor shall comply with any further written instructions with respect to processing by the Controller.
8. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	<p>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor in accordance with Clause 1.1.</p> <p>[Guidance: You may need to vary this section where (in the rare case) the Customer and Contractor have a different relationship. For example where the Parties are Joint Controller of some Personal Data:</p> <p>"Notwithstanding Clause 1.1 the Parties acknowledge that they are also Joint Controllers for the purposes of the Data Protection Legislation in respect of:</p> <p style="padding-left: 40px;">[Insert the scope of Personal Data which the purposes and means of the processing is determined by the both Parties]</p> <p>In respect of Personal Data under Joint Control, Clause 1.1-1.15 will not apply and the Parties agree to put in place a Joint Controller Agreement as outlined in Schedule Y instead."</p>
Subject matter of the processing	<p>[This should be a high level, short description of what the processing is about i.e. its subject matter of the contract.</p> <p>Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public.</p> <p>]</p>

Duration of the processing	[Clearly set out the duration of the processing including dates]
Nature and purposes of the processing	<p>[Please be as specific as possible, but make sure that you cover all intended purposes.</p> <p>The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</p> <p>The purpose might include: employment processing, statutory obligation, recruitment assessment etc]</p>
Type of Personal Data being Processed	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]
Categories of Data Subject	[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]
<p>Plan for return and destruction of the data once the processing is complete</p> <p>UNLESS requirement under union or member state law to preserve that type of data</p>	[Describe how long the data will be retained for, how it be returned or destroyed]

## SCHEDULE [Guidance: insert schedule ref here] SECURITY PROVISIONS

### 2. SECURITY PROVISIONS

#### 2.1 Definitions

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

<b>"Affiliates"</b>	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;
<b>"Breach of Security"</b>	in accordance with the Security Requirements and the Security Policy, the occurrence of: <ul style="list-style-type: none"> <li>(c) any unauthorised access to or use of the Works, the Employer Premises, the Sites, the Contractor System and/or any ICT, information or data (including the Confidential Information and the Employer Data) used by the Employer and/or the Contractor in connection with this Contract; and/or</li> <li>(d) 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 Contractor in connection with this Contract.</li> </ul>
<b>"Clearance"</b>	means national security clearance and employment checks undertaken by and/or obtained from the Defence Vetting Agency;
<b>"Contractor Equipment"</b>	the hardware, computer and telecoms devices and equipment supplied by the Contractor or its sub-contractors (but not hired, leased or loaned from the Employer) for the carrying out of the Works;
<b>"Contractor Software"</b>	software which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of carrying out of the Works;
<b>"Contractor System"</b>	the information and communications technology system used by the Contractor in carrying out of the Works including the Software, the Contractor Equipment and related cabling (but excluding the Employer System);
<b>"Control"</b>	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,

*Standard 'boilerplate' amendments*

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-contractors 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 parties;

**"Employer Premises"**

means premises owned, controlled or occupied by the Employer or its Affiliates which are made available for use by the Contractor or its sub-contractors for carrying out of the Works (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 Contractor in connection with this Contract which is owned by or licensed to the Employer by a third party and which interfaces with the Contractor System or which is necessary for the Employer to benefit from the Works;

**"Environmental Information Regulations"**

the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issued 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 Contractor System;

**"Impact Assessment"**

an assessment of a Change Request;

**"Information"**

has the meaning given under section 84 of the Freedom of Information Act 2000;

*Standard 'boilerplate' amendments*

<b>"Information Assets Register"</b>	the register of information assets to be created and maintained by the Contractor throughout the carrying out of the Works as described in the Contract (if any) or as otherwise agreed between the parties;
<b>"ISMS"</b>	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 Works;
<b>"Know-How"</b>	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the Works but excluding know how already in the Contractor's or the Employer's possession before this contract;
<b>"List x"</b>	means, in relation to a sub-contractor, one who has been placed on List x in accordance with Ministry of Defence guidelines and procedures, due to that sub-contractor undertaking work on its premises marked as CONFIDENTIAL or above;
<b>"Malicious Software"</b>	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;
<b>"Process"</b>	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;
<b>"Protectively Marked"</b>	shall have the meaning as set out in the Security Policy Framework.
<b>"Regulatory Bodies"</b>	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;
<b>"Request for Information"</b>	a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations;
<b>"Security Management Plan"</b>	the Contractor's security plan prepared pursuant to paragraph 1.5.3 of this schedule (Security Management Plan) an outline of which is set out in Appendix 1 of this schedule (Security Management Plan);
<b>"Security Policy"</b>	means the Cabinet Office Security Policy Framework (available

*Standard 'boilerplate' amendments*

<b>Framework"</b>	from the Cabinet Office Security Policy Division);
<b>"Security Requirements"</b>	means the requirements in the Contract relating to security of the carrying out of the Works (if any) or such other requirements as the Employer may notify to the Contractor from time to time
<b>"Security Tests"</b>	shall have the meaning set out in paragraph 2.4.1 of Part 2 of this Schedule (Security Management Plan);
<b>"Sites"</b>	any premises at which the Works are carried out or from which the Contractor manages, organises or otherwise directs the provision or the use of the Works or where any part of the Contractor System is situated or where any physical interface with the Employer System takes place;
<b>"Software"</b>	Specially Written Software, Contractor Software and Third Party Software;
<b>"Specially Written Software"</b>	any software created by the Contractor (or by a third party on behalf of the Contractor) specifically for the purposes of this contract;
<b>"Staff Vetting Procedures"</b>	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;
<b>"Statement of Applicability"</b>	shall have the meaning set out in ISO/IEC 27001 and as agreed by the parties during the procurement phase;
<b>"Standards"</b>	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;
<b>"Third Party Software"</b>	software which is proprietary to any third party other than an Affiliate of the Contractor which is or will be used by the Contractor for the purposes of carrying out of the Works; and

## 2.2 Introduction

### 2.2.1 This schedule covers:

- 2.2.1.1 principles of protective security to be applied in carrying out of the Works;
- 2.2.1.2 wider aspects of security relating to carrying out of the Works;

*Standard 'boilerplate' amendments*

- 2.2.1.3 the development, implementation, operation, maintenance and continual improvement of an ISMS;
- 2.2.1.4 the creation and maintenance of the Security Management Plan;
- 2.2.1.5 audit and testing of ISMS compliance with the Security Requirements;
- 2.2.1.6 conformance to ISO/IEC 27001 (Information Security Requirements Specification) and ISO/IEC27002 (Information Security Code of Practice) and;
- 2.2.1.7 obligations in the event of actual, potential or attempted breaches of security.

## 2.3 Principles of Security

- 2.3.1 The Contractor acknowledges that the Employer places great emphasis on the confidentiality, integrity and availability of information and consequently on the security provided by the ISMS.
- 2.3.2 The Contractor shall be responsible for the effective performance of the ISMS and shall at all times provide a level of security which:
  - 2.3.2.1 is in accordance with Good Industry Practice, the law of the Contract and this contract;
  - 2.3.2.2 complies with the Security Policy;
  - 2.3.2.3 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);
  - 2.3.2.4 meets any specific security threats to the ISMS; and
  - 2.3.2.5 complies with ISO/IEC27001 and ISO/IEC27002 in accordance with paragraph 1.3.2 of this schedule;
  - 2.3.2.6 complies with the Security Requirements; and
  - 2.3.2.7 complies with the Employer's ICT standards.
- 2.3.3 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.
- 2.3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Contractor gives an early warning to the Architect/Contract Administrator of such inconsistency immediately upon becoming aware of the same, and the Architect/Contract Administrator shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.

*Standard 'boilerplate' amendments*

2.4 ISMS and Security Management Plan

2.4.1 Introduction:

- 2.4.1.1 The Contractor shall develop, implement, operate, maintain and continuously improve and maintain an ISMS which will, without prejudice to paragraph 1.3.2, be approved, by the Architect/Contract Administrator, 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.
- 2.4.1.2 The Contractor shall develop and maintain a Security Management Plan in accordance with this Schedule to apply during the carrying out of the Works.
- 2.4.1.3 The Contractor shall comply with its obligations set out in the Security Management Plan.
- 2.4.1.4 Both the ISMS and the Security Management Plan shall, unless otherwise specified by the Employer, aim to protect all aspects of the Works and all processes associated with carrying out the Works, including the Affected Property, the Contractor 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 Contractor in connection with this contract.

2.4.2 Development of the Security Management Plan:

- 2.4.2.1 Within 20 Working Days after the Contract Date and in accordance with paragraph 1.4.4 (Amendment and Revision), the Contractor will prepare and deliver to the Architect/Contract Administrator for approval 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 Schedule.
- 2.4.2.2 If the Security Management Plan, or any subsequent revision to it in accordance with paragraph 1.4.4 (Amendment and Revision), is approved by the Architect/Contract Administrator 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. If the Security Management Plan is not approved by the Architect/Contract Administrator the Contractor shall amend it within 10 Working Days or such other period as the parties may agree in writing of a notice of non-approval from the Architect/Contract Administrator and re-submit to the Architect/Contract Administrator for approval. The parties will use all reasonable endeavours to ensure that the approval 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 Architect/Contract Administrator. If the Architect/Contract



*Standard 'boilerplate' amendments*

Administrator does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Architect/Contract Administrator pursuant to this paragraph 1.4.2.2 of this schedule may be unreasonably withheld or delayed. However any failure to approve 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.

2.4.3 Content of the Security Management Plan:

- 2.4.3.1 The Security Management Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Works and all processes associated with carrying out the Works and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Works comply with the provisions of this schedule (including the principles set out in paragraph 1.3);
- 2.4.3.2 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 Contractor's ISMS at the date notified by the Architect/Contract Administrator to the Contractor for the Contractor to meet the full obligations of the Security Requirements.
- 2.4.3.3 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.
- 2.4.3.4 The Security Management Plan shall be written in plain English in language which is readily comprehensible to the staff of the Contractor and the Employer engaged in the Works and shall only reference documents which are in the possession of the Employer or whose location is otherwise specified in this schedule.

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

- 2.4.4.1 The ISMS and Security Management Plan will be fully reviewed and updated by the Contractor annually or from time to time to reflect:
  - (a) emerging changes in Good Industry Practice;
  - (b) any change or proposed change to the Contractor System, the Works and/or associated processes;
  - (c) any new perceived or changed security threats; and
  - (d) any reasonable request by the Architect/Contract Administrator.

*Standard 'boilerplate' amendments*

- 2.4.4.2 The Contractor will provide the Architect/Contract Administrator 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.
- 2.4.4.3 On receipt of the results of such reviews, the Architect/Contract Administrator will approve any amendments or revisions to the ISMS or Security Management Plan in accordance with the process set out at paragraph 1.4.2.2.
- 2.4.4.4 Any change or amendment which the Contractor proposes to make to the ISMS or Security Management Plan (as a result of a Architect/Contract Administrator's request or change to the Works or otherwise) shall be subject to the early warning procedure and shall not be implemented until approved in writing by the Architect/Contract Administrator.
- 2.4.5 Testing
- 2.4.5.1 The Contractor shall conduct tests of the ISMS ("Security Tests") 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 Architect/Contract Administrator.
- 2.4.5.2 The Architect/Contract Administrator shall be entitled to witness the conduct of the Security Tests. The Contractor shall provide the Architect/Contract Administrator with the results of such tests (in a form approved by the Employer in advance) as soon as practicable after completion of each Security Test.
- 2.4.5.3 Without prejudice to any other right of audit or access granted to the Employer pursuant to this contract, the Architect/Contract Administrator and/or its authorised representatives shall be entitled, at any time and without giving notice to the Contractor, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Contractor's compliance with the ISMS and the Security Management Plan. The Architect/Contract Administrator may notify the Contractor of the results of such tests after completion of each such test. Security Tests shall be designed and implemented

*Standard 'boilerplate' amendments*

so as to minimise the impact on the carrying out the Works. If such tests adversely affect the Contractor's ability to carry out the Works in accordance with the Employer's Requirements, the Contractor shall be granted relief against any resultant under-performance for the period of the tests.

- 2.4.5.4 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 Contractor shall promptly notify the Architect/Contract Administrator of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to the Architect/Contract Administrator's approval in accordance with paragraph 1.4.1.1, the Contractor shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the Architect/Contract Administrator or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan to address a non-compliance with the Security Policy or Security Requirements the change to the ISMS or Security Management Plan shall be at no cost to the Employer.

2.5 Compliance with ISO/IEC 27001

- 2.5.1 Unless otherwise agreed by the parties, the Contractor shall obtain independent certification of the ISMS to ISO/IEC 27001 within 12 months of the Contract Date and shall maintain such certification for the duration of the contract.
- 2.5.2 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 Contractor reasonably believes that it is not compliant with ISO/IEC 27001, the Contractor shall promptly notify the Architect/Contract Administrator of this and the Employer in its absolute discretion may waive the requirement for certification in respect of the relevant parts.
- 2.5.3 The Architect/Contract Administrator 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.
- 2.5.4 If, on the basis of evidence provided by such audits, it is the Architect/Contract Administrator's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the Contractor, then the Architect/Contract Administrator shall notify the Contractor of the same and give the Contractor 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 Contractor does not become compliant within the required time then the Architect/Contract Administrator has the right to obtain an independent audit against these standards in whole or in part.

*Standard 'boilerplate' amendments*

- 2.5.5 If, as a result of any such independent audit as described in paragraph 1.5.4 the Contractor is found to be non-compliant with the principles and practices of ISO/IEC 27001 then the Contractor 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.
- 2.6 Breach of Security
- 2.6.1 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.
- 2.6.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 2.6.1, the Contractor shall:
- 2.6.2.1 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 Architect/Contract Administrator; and
- 2.6.2.2 as soon as reasonably practicable provide to the Architect/Contract Administrator 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**

*[Guidance Note: Append Security Policy]*

**Appendix 2 – Security Management Plan**

*[Guidance Note: Append Security Management Plan]*

**SCHEDULE** [Guidance: insert schedule ref here]

**CYBER ESSENTIALS**

**CYBER ESSENTIALS SCHEME**

**3. DEFINITIONS**

3.1 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.gov.uk/government/publications/cyber-essentials-scheme-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 Contractor 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 Contractor's cyber security approach under the Cyber Essentials Scheme and is a more advanced level of assurance.

**4. CYBER ESSENTIALS OBLIGATIONS**

2.1 Where the Employer's Requirements require that the Contractor provide a Cyber Essentials Certificate prior to the execution of the Works the Contractor shall provide a valid Cyber Essentials

Certificate, then on or prior to the commencement of the Works the Contractor delivers to the Employer evidence of the same. Where the Contractor fails to comply with this paragraph it shall be prohibited from commencing the carrying out of the works under any contract until such time as the Contractor has evidenced to the Employer its compliance with this paragraph 2.1.

2.2 Where the Contractor continues to Process Cyber Essentials Scheme Data during the carrying out of the works the Contractor shall deliver to the Employer evidence of renewal of the Cyber Essentials Certificate on each anniversary of the first applicable certificate obtained by the Contractor under paragraph 2.1.

2.3 Where the Contractor is due to Process Cyber Essentials Scheme Data after the commencement of the Works but before completion of the Works the Contractor shall deliver to the Employer evidence of:

2.3.1 a valid and current Cyber Essentials Certificate before the Contractor 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 Contractor under paragraph 2.1.

2.4 In the event that the Contractor 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 Contractor shall ensure that all sub-contracts with sub-contractors who Process Cyber Essentials Data contain provisions no less onerous on the sub-contractors than those imposed on the Contractor 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

## **SCHEDULE OF AMENDMENTS TO JCT MINOR WORKS BUILDING CONTRACT 2016 EDITION, JCT MINOR WORKS BUILDINGS CONTRACT WITHOUT CONTRACTOR'S DESIGN 2016 EDITION**

**ALL Clause references below will apply to all of the above forms**

**Insert** new article:

### **"Article 9: Schedule of Amendments**

The Contract is modified by the Schedule of Amendments (which has been initialled on behalf of both parties) and is to be read and construed accordingly."

*[Preparation Note: Unless an electronic version of the JCT contract is being used AND this new Article has been inserted in the text of it as an amendment, this new Article MUST be written, in manuscript, at the end of the Articles on the face of each original standard form JCT contract to be executed by the parties.]*

### **Clause 1.1. Definitions**

**Insert** the following new definitions:

"Commercially Sensitive Information: the information agreed between the parties (if any) comprising the information of a commercially sensitive nature relating to the Contractor, the charges for the Works, its IPR or its business or which the Contractor has indicated to the Employer that, if disclosed by the Employer, would cause the Contractor significant commercial disadvantage or material financial loss;

Confidential Information: the Employer's Confidential Information and/or the Contractor's Confidential Information;

Contracting Body: any Contracting Body as defined in Regulation 5(2) of the Public Contracts (Works, Service and Supply) (Amendment) Regulations 2000 other than the Employer.

Contractor's Confidential Information: any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and contractors of the Contractor, 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;

Crown Body: any department, office or agency of the Crown

Data Controller: has the meaning given to it in the Data Protection Act 2018

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.

Employer's Confidential Information: 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

Employer Data:

- 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 Contractor by or on behalf of the Employer; or
  - which the Contractor 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 Contractor.

Environmental Information Regulations: the Environmental Information Regulations 2004 and any guidance and/or codes of practice issued by the Information Commissioner 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 in relation to such legislation;

General Anti-Abuse Rule:

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

Halifax Abuse Principle: the principle explained in the CJEU Case C-255/02 Halifax and others

Intellectual Property Rights or "IPRs":

(a) 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;

(b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and

(c) all other rights having equivalent or similar effect in any country or jurisdiction;



Law: 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 Contractor is bound to comply;

Occasion of Tax Non-Compliance:

- where any tax return of the Contractor 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 Contractor 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;
- The failure of an avoidance scheme which the Contractor was involved in, and which was, or should have been, notified to a Relevant Tax Authority under DOTAS or any equivalent or similar regime; and/or

where any tax return of the Contractor 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.

Personal Data: the meaning given to it in the Data Protection Act 2018

Prohibited Act:

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.

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 Information Regulations

Relevant Requirements: 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

Relevant Tax Authority: HM Revenue & Customs, or, if applicable, a tax authority in the jurisdiction in which the Contractor is established.

Security Policy: the Employer's security policy attached as Appendix 1 to Schedule [Guidance: insert schedule ref here] (Security Policy) as may be updated from time to time"

### **1.5 Contracts (Rights of Third Parties) Act 1999**

1.5 In clause 1.5 **delete** "Notwithstanding any other provision of this Contract," and **insert** "Subject to the express rights of any person under any collateral warranty granted under the provisions of this Contract,"

**Insert** new clauses 1.9 to 1.16 as follows:

#### **"MoD DEFCON Requirements**

1.9 The MoD special terms and conditions in the form of DEFCONs and DEFORMs shall be incorporated into this Contract as detailed in Contract Schedule [Guidance: insert schedule ref here]

#### **Freedom of information**

1.10.1 The Contractor acknowledges that unless the Architect/Contract Administrator has notified the Contractor 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, FOIA and the Environmental Information Regulations. The Contractor shall co-operate with and assist the Employer so as to enable the Employer to comply with its information disclosure obligations.

1.10.2 The Contractor shall:

1.10.2.1 transfer to the Architect/Contract Administrator 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;

1.10.2.2 provide the Architect/Contract Administrator with a copy of all Information in its possession, or power in the form that the Architect/Contract Administrator shall require within five Working Days (or such other period as the Architect/Contract Administrator may specify) of the Architect/Contract Administrator's request;

1.10.2.3 provide all necessary assistance as reasonably requested by the Architect/Contract Administrator 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

1.10.2.4 procures that its sub-contractors do likewise.

1.10.3 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.

1.10.4 The Contractor shall not respond directly to a Request for Information unless authorised to do so by the Architect/Contract Administrator.

1.10.5 The Contractor 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 Contractor or despite the Contractor having expressed negative views when consulted.

1.10.6 The Contractor shall ensure that all Information is retained for disclosure for twelve years where this Contract is executed as a deed or six years where this Contract is executed under hand and shall permit the Architect/Contract Administrator to inspect such records as and when reasonably requested from time to time."

#### **1.11 Tax Compliance**

1.11.1 The Contractor represents and warrants that as at the date of this Contract, 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.

1.11.2 If, at any point prior to the end of the Rectification Period, an Occasion of Tax Non-Compliance occurs, the Contractor shall:

1.11.2.1 notify the Employer in writing of such fact within 5 days of its occurrence; and

1.11.2.2 promptly provide to the Employer:

1.11.2.2.1 details of the steps which the Contractor 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

1.11.2.2.2 such other information in relation to the Occasion of Tax Non-Compliance as the Employer may reasonably require.

## 1.12 GDPR

The Employer and the Contractor shall comply with the provisions of schedule [Guidance: insert schedule ref here]

## 1.13 Confidentiality and Information Sharing

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

1.13.1.1 treat the other party's Confidential Information as confidential and safeguard it accordingly; and

1.13.1.2 not disclose the other party's Confidential Information to any other person without the owner's prior written consent.

1.13.1.3 immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information

1.13.1.4 notify the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010

1.13.2 The clause above shall not apply to the extent that:

1.13.2.1 such disclosure is a requirement of the law of the contract placed upon the party making the disclosure, including any requirements for disclosure under the FOIA or the Environmental Information Regulations pursuant to clause 1.10 (Freedom of Information);

1.13.2.2 such information was in the possession of the party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;

1.13.2.3 such information was obtained from a third party without obligation of confidentiality;

1.13.2.4 such information was already in the public domain at the time of disclosure otherwise than by a breach of this Contract; or

1.13.2.5 it is independently developed without access to the other party's Confidential Information.

1.13.3 The Contractor may only disclose the Employer's Confidential Information to Contractor's Persons who are directly involved in the provision of the service and who need to know the information, and shall ensure that such Contractor's Persons are aware of and shall comply with these obligations as to confidentiality.

1.13.4 The Contractor shall not, and shall procure that the Contractor's Persons do not, use any of the Employer's Confidential Information received otherwise than for the purposes of this contract.

1.13.5 The Contractor may only disclose the Employer's Confidential Information to Contractor's Persons who need to know the information, and shall ensure that such Contractor's Persons 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 Contractor's Persons causes or contributes (or could cause or contribute) to the Contractor breaching its obligations as to confidentiality under or in connection with this contract, the Contractor 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 Contractor Personnel, the Contractor 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 Contractor is taking appropriate steps to comply with this clause, including copies of any written communications to and/or from Contractor's Persons, and any minutes of meetings and any other records which provide an audit trail of any discussions or exchanges with Contractor's Persons in connection with obligations as to confidentiality.

1.13.6 At the written request of the Employer, the Contractor shall procure that those members of the Contractor's Persons identified in the Employer's notice signs a confidentiality undertaking prior to commencing any work in accordance with this Contract.

1.13.7 Nothing in this Contract shall prevent the Employer from disclosing the Contractor's Confidential Information:

1.13.7.1 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 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;

1.13.7.2 to any consultant, contractor or other person engaged by the Employer or any person conducting an Office of Government Commerce gateway review;

1.13.7.3 for the purpose of the examination and certification of the Employer's accounts; or

1.13.7.4 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.

and for the purposes of the foregoing, disclosure of the Contractor'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 1.13.

1.13.8 The Employer shall use all reasonable endeavours to ensure that any government department, Contracting Body, employee, third party or sub-contractor to whom the Contractor's Confidential Information is disclosed pursuant to the above clause is made aware of the Employer's obligations of confidentiality.

1.13.9 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

1.13.10 The Employer may disclose the Confidential Information of the Contractor:

1.13.10.1 on a confidential basis to any Crown Body for any proper purpose of the Employer or the relevant Crown Body;

1.13.10.2 to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;

1.13.10.3 to the extent that the Employer (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;

1.13.10.4 on a confidential basis to a professional adviser, consultant, supplier or other person engaged by any Crown Body (including any benchmarking organisation) for any purpose connected with this Contract;

1.13.10.5 on a confidential basis for the purpose of the exercise of its rights under this Contract;

1.13.10.6 on a confidential basis 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, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Employer under this clause.

#### **1.14 Prevention of Fraud and Bribery**

1.14.1 The Contractor represents and warrants that neither it, nor to the best of its knowledge any of its employees, have at any time prior to the date of this Contract:

1.14.1.1 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

1.14.1.2 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.

1.14.2 During the carrying out of the Works the Contractor shall not:

1.14.2.1 commit a Prohibited Act; and/or

1.14.2.2 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

1.14.3 During the carrying out of the Works the Contractor shall:

1.14.3.1 establish, maintain and enforce, and require that its sub-contractors 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;

1.14.3.2 keep appropriate records of its compliance with this Contract and make such records available to the Employer on request;

1.14.3.3 provide and maintain and where appropriate enforce an anti-bribery policy (which shall be disclosed to the Employer on request) to prevent it and any Contractor's employees or any person acting on the Contractor's behalf from committing a Prohibited Act.

1.14.4 The Contractor shall notify the Employer immediately in writing if it becomes aware of any breach of clause 1.14.1, or has reason to believe that it has or any of its employees or sub-contractors have:

1.14.4.1 been subject to an investigation or prosecution which relates to an alleged Prohibited Act;

1.14.4.2 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; and/or

1.14.4.3 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.

1.14.5 If the Contractor shall make a notification to the Employer pursuant to clause 1.14.4, the Contractor shall respond promptly to the Employer's enquiries, co-operate with any investigation, and allow the Employer to audit any books, records and/or any other relevant documentation in accordance with this Contract.

1.14.6 If the Contractor breaches Clause 1.14.3, the Employer may by notice require the Contractor to remove from carrying out the Works any Contractor's Person whose acts or omissions have caused the Contractor's breach.

### **1.15 Security requirements**

The Contractor shall comply with, and procure the compliance of the Contractor's Persons, with:

1.15.1 the Security Policy and the Security Management Plan and the Contractor shall ensure that the Security Management Plan produced by the Contractor fully complies with the Security Policy;

1.15.2 Contract Schedule [Guidance: insert schedule ref here] (Security Provisions).

### **1.16 Cyber Essentials**

The Employer and the Contractor shall comply with the provisions of schedule [Guidance: insert schedule ref here] "

### **2.1 Contractor's obligations**

**Insert** new clauses 2.1A to 2.1D as follows:

#### **"2.1A Admittance to the site**

2.1.A.1 The Contractor shall submit details of people who are to be employed by it and its sub-contractors in connection with the Works to the Architect/Contract Administrator. The details shall include a list of names and addresses, the capabilities in which they are employed, and other information required by the Architect/Contract Administrator.

2.1.A.2 The Architect/Contract Administrator may instruct the Contractor to take measures to prevent unauthorised persons being admitted to site. The instruction shall be valued as a variation under clause 3.6.1 if the measures are additional to those required by the Employer's Requirements.

2.1.A.3 Contractor's Persons are to carry an Employer's pass and comply with all conduct requirements from the Employer whilst they are on the parts of the site identified in the Employer's Requirements.

2.1.A.4 The Contractor shall submit to the Architect/Contract Administrator for acceptance a list of the names of the people for whom passes are required. On acceptance, the Architect/Contract Administrator will issue the passes to the Contractor. Each pass shall be returned to the Architect/Contract Administrator when the employee no longer requires access to that part of the site or after the Architect/Contract Administrator has given notice that the employee is not to be admitted to the site.



2.1.A.5 The Contractor shall not take photographs of the site or of work carried out in connection with the Works unless it has obtained the acceptance of the Architect/Contract Administrator.

2.1.A.6 The Contractor shall take the measures needed to prevent any Contractor's Persons taking, publishing or otherwise circulating such photographs

#### **2.1.B Legislation and Official secrets**

2.1.B.1 The Contractor shall comply with the Law in the carrying out of the Works.

2.1.B.2 The Official Secrets Acts 1911 to 1989 and, where appropriate, the provisions of section 11 of the Atomic Energy Act 1946 apply to this Contract.

2.1.B.3 The Contractor shall notify its employees and its sub-contractors of their duties under these Acts.

#### **2.1.C Building Information Modelling**

2.1.C.1 A BIM Protocol applies/does not apply [delete as appropriate]

2.1.C.2 When a BIM Protocol applies it is detailed in the Employer's Information Requirements

2.1.C.3 When the CIC Building Information Modelling Protocol applies clauses 2.1.C.4 to 2.1.C.6.2 shall apply

2.1.C.4 In this clause, the Protocol is the CIC Building Information Modelling Protocol, first edition 2013. Terms used in this clause are those defined in the Protocol.

2.1.C.5 Clauses 1, 2, 5, 6, 7 of the Protocol shall form part of this Contract. Clauses 3 and 4 and Appendices 1 and 2 of the Protocol are deemed to be part of the Client's Requirements.

2.1.C.6: The following shall be deemed to be a Change:

2.1.C.6.1 If the Constructor encounters an event which is outside his reasonable control and which prevents him from carrying out the work specified in clause 4.1.2 of the Protocol.

2.1.C.6.2 If the Client revokes a licence granted under clause 6.6 of the Protocol.

2.1D In this clause 2.1D only:

**"Intellectual Property Rights"** means any and all patents, trademarks, service marks, copyright, moral rights, rights in a design, know-how, Confidential Information and all or any other intellectual or industrial property rights whether or not registered or capable of registration and whether subsisting in the United Kingdom or any other part of the world together with all or any goodwill relating or attached thereto;

**"Confidential Information"** means any information designated as such by the Party disclosing that information; and

**"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 Contractor in relation to this Contract.



2.1D.1 The Intellectual Property Rights in all Documents prepared by or on behalf of the Contractor in relation to this Contract and the work executed from them remains the property of the Contractor. The Contractor 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 Site. Such licence entitles the Employer to grant sub-licences to third parties in the same terms as this licence provided always that the Contractor shall not be liable to any licensee for any use of the Documents or the Intellectual Property Rights in the Documents for purposes other than those for which the same were originally prepared by or on behalf of the Contractor.

2.1D.2 The Employer may assign, novate or otherwise transfer its rights and obligations under the licence granted pursuant to 2.1D.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.

2.1D.3 In the event that the Contractor does not own the copyright or any Intellectual Property Rights in any Document the Contractor shall use 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 Contractor is unable to procure the right to grant to the Employer in accordance with the foregoing the Contractor shall procure that the third party grants a direct licence to the Employer on industry acceptable terms.

2.1D.4 The Contractor 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.

2.1D.5 In the event that any act unauthorised by the Employer infringes a moral right of the Contractor in relation to the Documents the Contractor undertakes, if the Employer so requests and at the Employer's expense, to institute proceedings for infringement of the moral rights.

2.1D.6 The Contractor warrants to the Employer that he 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.

2.1D.7 The Contractor shall supply copies of the Documents to the Architect/Contract Administrator 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 works.

2.1D.8 After the termination or conclusion of the Contractor's employment hereunder, the Contractor shall supply the Architect/Contract Administrator with copies and/or computer discs of such of the Documents as the Architect/Contract Administrator may from time to time request and the Employer shall pay the Contractor's reasonable costs for producing such copies or discs.

2.1D.9 In carrying out the Works the Contractor shall not infringe any Intellectual Property Rights of any third party. The Contractor shall indemnify the Employer against claims, proceedings, compensation and costs arising from an infringement or alleged infringement of the Intellectual Property Rights of any third party.

### 3.3 Sub-contracting

3.3.2.4 to 3.3.2.7 **Insert** new subclauses 3.3.2.4 to 3.3.2.7 as follows:

"3.3.2.4 a period for payment of the amount due to the sub-contractor not greater than 5 days after the final date for payment in this Contract. The amount due shall, but shall not be limited to, payment for work which the sub-contractor has completed from the previous application date up to the current application date in this Contract;

3.3.2.5 a provision requiring the sub-contractor 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

3.3.2.6 a provision requiring the sub-contractor to assess the amount due to a subsubcontractor without taking into account the amount paid by the Contractor.

3.3.2.7 terms and conditions that are no less favourable than those of this Contract. The Employer shall be entitled to reject sub-contract conditions proposed by the Contractor that are unduly disadvantageous to the sub-contractor"

3.6A **Insert** new clause 3.6A

"3.3A.1 The Contractor shall take all reasonable steps to engage SMEs as sub-contractors and to seek to ensure that no less than the percentage of the sub-contractors stated in the Employer's Requirements (the "SME Percentage") are SMEs or that a similar proportion of the Contract Sum is undertaken by SMEs.

3.3A.2 The Contractor shall report to the Employer on a monthly basis the numbers of SMEs engaged as sub-contractors and the value of the Contract Sum that has been undertaken by SMEs.

3.3A.3 Where available, the Contractor shall tender its sub-contracts using the same online electronic portal as was provided by the Employer for the purposes of tendering this Contract.

3.3B **Insert** new clause 3.3B as follows:

#### "3.3B Apprenticeships

3.3B.1 The Contractor shall take all reasonable steps to employ apprentices, and report to the Employer the numbers of apprentices employed and the wider skills training provided, during the carrying out of the Works.

3.3B.2 The Contractor shall take all reasonable steps to ensure that no less than the percentage of its employees stated in the Employer's Requirements (the "Apprenticeship Percentage") are on formal apprenticeship programmes or that a similar proportion of hours worked in carrying out the Works, (which may include support staff and sub-contractors) are provided by employees on formal apprenticeship programmes.

3.3B.3 The Contractor shall make available to its employees and sub-contractors working on the Contract, information about the Government's Apprenticeship programme and wider skills opportunities.

3.3B.4 The Contractor shall provide any further skills training opportunities that are appropriate for its employees engaged in carrying out the Works.

3.3B.5 The Contractor shall provide a written report detailing the following measures in its regular contract management monthly reporting cycle and be prepared to discuss apprenticeships at its regular meetings with the Architect/Contract Administrator:

- the number of people during the reporting period employed on the Contract, including support staff and sub-contractors;
- the number of apprentices and number of new starts on apprenticeships directly initiated through the procurement process;
- the percentage of all employees taking part in an apprenticeship programme;
- if applicable, an explanation from the Contractor as to why it is not managing to meet the specified percentage target;
- actions being taken to improve the take up of apprenticeships;
- other training/skills development being undertaken by employees 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."

**Insert** new clause 4A as follows:

#### **"4A Project Bank Account**

The parties shall comply with the provisions of Schedule [Guidance: insert schedule ref here] "

**SCHEDULE** [Guidance: insert schedule ref here]

**PROJECT BANK**

## **ACCOUNT**

### **1. Definitions**

The following definitions shall apply to this Schedule

Authorisation: a document authorising the Project Bank to make payments to the Contractor and Named Suppliers.

Named Suppliers: such Suppliers as are detailed in the Employer's Requirements and such other Suppliers who have signed the Joining Deed.

Project Bank: such bank as the Employer shall inform the Contractor in writing

Project Bank Account: the account used to receive payments from the Employer and to make payments to the Contractor and Named Suppliers

A Suppliers: a person or organisation who has a contract to

- construct or install part of the Works,
- provide a service necessary to provide the Works or
- supply Plant and Materials for the Works.

Trust Deed: an agreement in the form set out in the Contract which contains provisions for administering the Project Bank Account.

Joining Deed: an agreement in the form set out in the Contract under which the Supplier joins the Trust Deed.

### **2. Project Bank Account**

2.1 The Employer shall establish the Project Bank Account with the Project Bank within three weeks of the date of this Contract.

2.2 Unless stated otherwise in the Employer's Requirements, the Employer shall pay any charges made and is paid any interest paid by the Project Bank. The charges and interest by the Project Bank are not included in the Contract Sum.

### **3. Named Suppliers**

The Contractor shall include in its contracts with Named Suppliers the arrangements in the contract for the operation of the Project Bank Account and Trust Deed. The Contractor shall inform the Named Suppliers of the details of the Project Bank Account and the arrangements for payment of amounts due under their contracts.

### **4. Payments**

4.1 The Contractor shall submit proposals for adding a Supplier to the Suppliers to the Architect/Contract Administrator for acceptance. A reason for not accepting is that the addition of such Supplier would not comply with the Employer's Requirements. The Employer, the Contractor and the Supplier shall sign the Joining Deed after acceptance

4.2 The Contractor shall show in the application for payment the amounts due to Named Suppliers in accordance with their contracts.

4.3 Within the time set out in the banking arrangements to allow the Project Bank to make payment to the Contractor and Named Suppliers in accordance with the Contract, the Employer shall make payment to the Project Bank Account of the amount which is due to be paid under the Contract

4.4 The Contractor shall prepare the Authorisation, setting out the sums due to Named Suppliers as assessed by the Contractor and to the Contractor for the balance of the payment due under the Contract. After signing the Authorisation, the Contractor shall submit it to the Architect/Contract Administrator no later than four days before the final date for payment. The Employer shall sign the Authorisation and submit it to the Project Bank no later than one day before the final date for payment.

4.5 The Contractor and Named Suppliers shall receive payment from the Project Bank Account of the sums set out in the Authorisation as soon as practicable after the Project Bank Account receives payment.

4.6 Any payment which is due from the Contractor to the Employer shall not be made through the Project Bank Account

## **5. Effect of Payment**

Payments made from the Project Bank Account are treated as payments from the Employer to the Contractor in accordance with the Contract or from the Contractor or Supplier to Named Supplier in accordance with their contracts as applicable. A delay in payment due to a failure of the Contractor to comply with the requirements of this clause is not treated as late payment under the Contract.

## **6. Trust Deed**

The Employer, the Contractor and Named Suppliers shall sign the Trust Deed before the first Interim Valuation Date.

## **7. Termination**

If the Architect/Contract Administrator issues a termination certificate, no further payment is to be made into the Project Bank Account.

## FORM OF TRUST DEED

This agreement is made between the "**Employer**", the "**Contractor**" and the Named Suppliers.

Terms in this deed have the meanings given to them in the contract between  
and for ("**Works**").

### BACKGROUND

The Employer and the Contractor have entered into a contract for the Works.

The Named Suppliers have entered into contracts with the Contractor or a subcontractor in connection with the Works.

The Contractor has established a Project Bank Account to make provision for payment to the Contractor and the Named Suppliers.

### AGREEMENT

The parties to this deed agree that:

4. sums due to the Contractor and Named Suppliers and set out in the Authorisation are held in trust in the Project Bank Account by the Contractor for distribution to the Contractor and Named Suppliers in accordance with the banking arrangements applicable to the Project Bank Account.
5. Further Named Suppliers may be added as parties to this deed with the agreement of the Employer and Contractor. The agreement of the Employer and Contractor is treated as agreement by the Named Suppliers who are parties to this deed.
6. This deed is subject to the law of the contract for the Works.
7. The benefits under this deed may not be assigned.

Executed as a deed, but not delivered until the )  
first date specified on page 1 by )  
:

Signature .....

Name (block capitals) .....

**Employer**

*Standard 'boilerplate' amendments*

Signature .....

Name (block capitals) .....

**Contractor**

Signature .....

Name (block capitals) .....

**Supplier**



## FORM OF JOINING DEED

-----  
This agreement is made between the "**Employer**", the "**Contractor**" and  
("**Additional Supplier**").

Terms in this deed have the meanings given to them in the contract between  
and for ("**Works**").

### BACKGROUND

The Employer and the Contractor have entered into a contract for the Works.

The Named Suppliers have entered into contracts with the Contractor or a sub-contractor in  
connection with the Works.

The Contractor has established a Project Bank Account to make provision for payment to the  
Contractor and the Named Suppliers.

The Employer, the Contractor and the Named Suppliers have entered into a deed as set out in  
Annex 1 ("**Trust Deed**"), and have agreed that the Additional Supplier may join that deed.

### AGREEMENT

The parties to this deed agree that:

8. The Additional Supplier becomes a party to the Trust Deed from the date set out below.
9. This deed is subject to the law of the contract for the Works.
10. The benefits under this deed may not be assigned.

Executed as a deed, but not delivered until the )  
first date specified on page 1 by )  
:

Signature \_\_\_\_\_

Name (block capitals) \_\_\_\_\_

**Employer**

Signature

*Standard 'boilerplate' amendments*

Name (block capitals) \_\_\_\_\_  
**Contractor**

Signature \_\_\_\_\_

Name (block capitals) \_\_\_\_\_  
**Additional Supplier**

**SCHEDULE** [Guidance: insert schedule ref here]

**GDPR**

The following definitions shall apply to this Schedule [Guidance: insert schedule ref here]

**Party** : a Party to this Agreement

**Agreement** : this contract;

**Law** : means any law, 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, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply;

**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, the LED and any applicable national implementing Laws as amended from time to time (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;

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 GDPR.

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)

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

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

Protective Measures : appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule [x] (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 Contractor is the Processor unless otherwise specified in Schedule

[X]. The only processing that the Processor is authorised to do is listed in Schedule [X] 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 [ X ], unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;
- (b) ensure that it has in place Protective Measures, are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:
  - (i) nature of the data to be protected;
  - (ii) harm that might result from a Data Loss Event;
  - (iii) state of technological development; and
  - (iv) cost of implementing any measures;
- (c) ensure that :
  - (i) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule X);
  - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

- (A) are aware of and comply with the Processor's duties under this clause;
- (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
- (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and
- (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
- (d) not transfer Personal Data outside of the EU 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 (whether in accordance with GDPR Article 46 or LED Article 37) 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 [X] 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 [X] 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 [X] 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.

9. The contact details of the Controller's Data Protection Officer are: [Insert Contact details]
10. The contact details of the Processor's Data Protection Officer are: [Insert Contact details]
11. The Processor shall comply with any further written instructions with respect to processing by the Controller.
12. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	<p>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor in accordance with Clause 1.1.</p> <p>[Guidance: You may need to vary this section where (in the rare case) the Customer and Contractor have a different relationship. For example where the Parties are Joint Controller of some Personal Data:</p> <p>"Notwithstanding Clause 1.1 the Parties acknowledge that they are also Joint Controllers for the purposes of the Data Protection Legislation in respect of:</p> <p style="padding-left: 40px;">[Insert the scope of Personal Data which the purposes and means of the processing is determined by the both Parties]</p> <p>In respect of Personal Data under Joint Control, Clause 1.1-1.15 will not apply and the Parties agree to put in place a Joint Controller Agreement as outlined in Schedule Y instead."</p>
Subject matter of the processing	<p>[This should be a high level, short description of what the processing is about i.e. its subject matter of the contract.</p> <p>Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public.</p> <p>]</p>

Duration of the processing	[Clearly set out the duration of the processing including dates]
Nature and purposes of the processing	<p>[Please be as specific as possible, but make sure that you cover all intended purposes.</p> <p>The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</p> <p>The purpose might include: employment processing, statutory obligation, recruitment assessment etc]</p>
Type of Personal Data being Processed	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]
Categories of Data Subject	[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]
<p>Plan for return and destruction of the data once the processing is complete</p> <p>UNLESS requirement under union or member state law to preserve that type of data</p>	[Describe how long the data will be retained for, how it be returned or destroyed]



## SCHEDULE [Guidance: insert schedule ref here] SECURITY PROVISIONS

### 3. SECURITY PROVISIONS

#### 3.1 Definitions

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

<b>"Affiliates"</b>	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;
<b>"Breach of Security"</b>	in accordance with the Security Requirements and the Security Policy, the occurrence of: <ul style="list-style-type: none"> <li>(e) any unauthorised access to or use of the Works, the Employer Premises, the Sites, the Contractor System and/or any ICT, information or data (including the Confidential Information and the Employer Data) used by the Employer and/or the Contractor in connection with this Contract; and/or</li> <li>(f) 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 Contractor in connection with this Contract.</li> </ul>
<b>"Clearance"</b>	means national security clearance and employment checks undertaken by and/or obtained from the Defence Vetting Agency;
<b>"Contractor Equipment"</b>	the hardware, computer and telecoms devices and equipment supplied by the Contractor or its sub-contractors (but not hired, leased or loaned from the Employer) for the carrying out of the Works;
<b>"Contractor Software"</b>	software which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of carrying out of the Works;
<b>"Contractor System"</b>	the information and communications technology system used by the Contractor in carrying out of the Works including the Software, the Contractor Equipment and related cabling (but excluding the Employer System);
<b>"Control"</b>	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,

*Standard 'boilerplate' amendments*

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-contractors 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 parties;

**"Employer Premises"**

means premises owned, controlled or occupied by the Employer or its Affiliates which are made available for use by the Contractor or its sub-contractors for carrying out of the Works (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 Contractor in connection with this Contract which is owned by or licensed to the Employer by a third party and which interfaces with the Contractor System or which is necessary for the Employer to benefit from the Works;

**"Environmental Information Regulations"**

the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issued 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 Contractor System;

**"Impact Assessment"**

an assessment of a Change Request;

**"Information"**

has the meaning given under section 84 of the Freedom of Information Act 2000;

*Standard 'boilerplate' amendments*

<b>"Information Assets Register"</b>	the register of information assets to be created and maintained by the Contractor throughout the carrying out of the Works as described in the Contract (if any) or as otherwise agreed between the parties;
<b>"ISMS"</b>	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 Works;
<b>"Know-How"</b>	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the Works but excluding know how already in the Contractor's or the Employer's possession before this contract;
<b>"List x"</b>	means, in relation to a sub-contractor, one who has been placed on List x in accordance with Ministry of Defence guidelines and procedures, due to that Sub contractor undertaking work on its premises marked as CONFIDENTIAL or above;
<b>"Malicious Software"</b>	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;
<b>"Process"</b>	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;
<b>"Protectively Marked"</b>	shall have the meaning as set out in the Security Policy Framework.
<b>"Regulatory Bodies"</b>	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;
<b>"Request for Information"</b>	a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations;
<b>"Security Management Plan"</b>	the Contractor's security plan prepared pursuant to paragraph 1.5.3 of this Schedule (Security Management Plan) an outline of which is set out in Appendix 1 of this schedule (Security Management Plan);
<b>"Security Policy"</b>	means the Cabinet Office Security Policy Framework (available

*Standard 'boilerplate' amendments*

<b>Framework"</b>	from the Cabinet Office Security Policy Division);
<b>"Security Requirements"</b>	means the requirements in the Contract relating to security of the carrying out of the Works (if any) or such other requirements as the Employer may notify to the Contractor from time to time
<b>"Security Tests"</b>	shall have the meaning set out in paragraph 2.4.1 of Part 2 of this Schedule (Security Management Plan);
<b>"Sites"</b>	any premises at which the Works are carried out or from which the Contractor manages, organises or otherwise directs the provision or the use of the Works or where any part of the Contractor System is situated or where any physical interface with the Employer System takes place;
<b>"Software"</b>	Specially Written Software, Contractor Software and Third Party Software;
<b>"Specially Written Software"</b>	any software created by the Contractor (or by a third party on behalf of the Contractor) specifically for the purposes of this contract;
<b>"Staff Vetting Procedures"</b>	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;
<b>"Statement of Applicability"</b>	shall have the meaning set out in ISO/IEC 27001 and as agreed by the parties during the procurement phase;
<b>"Standards"</b>	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;
<b>"Third Party Software"</b>	software which is proprietary to any third party other than an Affiliate of the Contractor which is or will be used by the Contractor for the purposes of carrying out of the Works; and

### 3.2 Introduction

#### 3.2.1 This schedule covers:

- 3.2.1.1 principles of protective security to be applied in carrying out of the Works;
- 3.2.1.2 wider aspects of security relating to carrying out of the Works;
- 3.2.1.3 the development, implementation, operation, maintenance and continual improvement of an ISMS;
- 3.2.1.4 the creation and maintenance of the Security Management Plan;
- 3.2.1.5 audit and testing of ISMS compliance with the Security Requirements;
- 3.2.1.6 conformance to ISO/IEC 27001 (Information Security Requirements Specification) and ISO/IEC27002 (Information Security Code of Practice) and;
- 3.2.1.7 obligations in the event of actual, potential or attempted breaches of security.

### 3.3 Principles of Security

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

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

- 3.3.2.1 is in accordance with Good Industry Practice, the law of the Contract and this contract;
- 3.3.2.2 complies with the Security Policy;
- 3.3.2.3 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);
- 3.3.2.4 meets any specific security threats to the ISMS; and
- 3.3.2.5 complies with ISO/IEC27001 and ISO/IEC27002 in accordance with paragraph 1.3.2 of this schedule;
- 3.3.2.6 complies with the Security Requirements; and
- 3.3.2.7 complies with the Employer's ICT standards.

*Standard 'boilerplate' amendments*

- 3.3.3 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.
- 3.3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Contractor gives an early warning to the Architect/Contract Administrator of such inconsistency immediately upon becoming aware of the same, and the Architect/Contract Administrator shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.
- 3.4 ISMS and Security Management Plan
- 3.4.1 Introduction:
- 3.4.1.1 The Contractor shall develop, implement, operate, maintain and continuously improve and maintain an ISMS which will, without prejudice to paragraph 1.3.2, be approved, by the Architect/Contract Administrator, 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.
- 3.4.1.2 The Contractor shall develop and maintain a Security Management Plan in accordance with this Schedule to apply during the carrying out of the Works.
- 3.4.1.3 The Contractor shall comply with its obligations set out in the Security Management Plan.
- 3.4.1.4 Both the ISMS and the Security Management Plan shall, unless otherwise specified by the Employer, aim to protect all aspects of the Works and all processes associated with carrying out the Works, including the Affected Property, the Contractor 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 Contractor in connection with this contract.
- 3.4.2 Development of the Security Management Plan:
- 3.4.2.1 Within 20 Working Days after the Contract Date and in accordance with paragraph 1.4.4 (Amendment and Revision), the Contractor will prepare and deliver to the Architect/Contract Administrator for approval 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 Schedule.
- 3.4.2.2 If the Security Management Plan, or any subsequent revision to it in accordance with paragraph 1.4.4 (Amendment and Revision), is approved by the Architect/Contract Administrator it will be adopted immediately and will replace the previous version of the Security

*Standard 'boilerplate' amendments*

Management Plan at Appendix 2 of this Part 2 of this Contract Schedule. If the Security Management Plan is not approved by the Architect/Contract Administrator the Contractor shall amend it within 10 Working Days or such other period as the parties may agree in writing of a notice of non-approval from the Architect/Contract Administrator and re-submit to the Architect/Contract Administrator for approval. The parties will use all reasonable endeavours to ensure that the approval 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 Architect/Contract Administrator. If the Architect/Contract Administrator does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Architect/Contract Administrator pursuant to this paragraph 1.4.2.2 of this schedule may be unreasonably withheld or delayed. However any failure to approve 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.

3.4.3 Content of the Security Management Plan:

- 3.4.3.1 The Security Management Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Works and all processes associated with carrying out the Works and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Works comply with the provisions of this schedule (including the principles set out in paragraph 1.3);
- 3.4.3.2 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 Contractor's ISMS at the date notified by the Architect/Contract Administrator to the Contractor for the Contractor to meet the full obligations of the Security Requirements.
- 3.4.3.3 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.
- 3.4.3.4 The Security Management Plan shall be written in plain English in language which is readily comprehensible to the staff of the Contractor and the Employer engaged in the Works and shall only reference documents which are in the possession of the Employer or whose location is otherwise specified in this schedule.

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



*Standard 'boilerplate' amendments*

- 3.4.4.1 The ISMS and Security Management Plan will be fully reviewed and updated by the Contractor annually or from time to time to reflect:
- (a) emerging changes in Good Industry Practice;
  - (b) any change or proposed change to the Contractor System, the Works and/or associated processes;
  - (c) any new perceived or changed security threats; and
  - (d) any reasonable request by the Architect/Contract Administrator.
- 3.4.4.2 The Contractor will provide the Architect/Contract Administrator 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.
- 3.4.4.3 On receipt of the results of such reviews, the Architect/Contract Administrator will approve any amendments or revisions to the ISMS or Security Management Plan in accordance with the process set out at paragraph 1.4.2.2.
- 3.4.4.4 Any change or amendment which the Contractor proposes to make to the ISMS or Security Management Plan (as a result of a Architect/Contract Administrator's request or change to the Works or otherwise) shall be subject to the early warning procedure and shall not be implemented until approved in writing by the Architect/Contract Administrator.
- 3.4.5 Testing
- 3.4.5.1 The Contractor shall conduct tests of the ISMS ("Security Tests") 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 Architect/Contract Administrator.
- 3.4.5.2 The Architect/Contract Administrator shall be entitled to witness the conduct of the Security Tests. The Contractor shall provide the



### *Standard 'boilerplate' amendments*

Architect/Contract Administrator with the results of such tests (in a form approved by the Employer in advance) as soon as practicable after completion of each Security Test.

- 3.4.5.3 Without prejudice to any other right of audit or access granted to the Employer pursuant to this contract, the Architect/Contract Administrator and/or its authorised representatives shall be entitled, at any time and without giving notice to the Contractor, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Contractor's compliance with the ISMS and the Security Management Plan. The Architect/Contract Administrator may notify the Contractor 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 the Works. If such tests adversely affect the Contractor's ability to carry out the Works in accordance with the Employer's Requirements, the Contractor shall be granted relief against any resultant under-performance for the period of the tests.
- 3.4.5.4 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 Contractor shall promptly notify the Architect/Contract Administrator of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to the Architect/Contract Administrator's approval in accordance with paragraph 1.4.1.1, the Contractor shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the Architect/Contract Administrator or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan to address a non-compliance with the Security Policy or Security Requirements the change to the ISMS or Security Management Plan shall be at no cost to the Employer.

## 3.5 Compliance with ISO/IEC 27001

- 3.5.1 Unless otherwise agreed by the parties, the Contractor shall obtain independent certification of the ISMS to ISO/IEC 27001 within 12 months of the Contract Date and shall maintain such certification for the duration of the contract.
- 3.5.2 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 Contractor reasonably believes that it is not compliant with ISO/IEC 27001, the Contractor shall promptly notify the Architect/Contract Administrator of this and the Employer in its absolute discretion may waive the requirement for certification in respect of the relevant parts.
- 3.5.3 The Architect/Contract Administrator shall be entitled to carry out such regular security audits as may be required and in accordance with Good Industry Practice,

### Standard 'boilerplate' amendments

in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001.

3.5.4 If, on the basis of evidence provided by such audits, it is the Architect/Contract Administrator's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the Contractor, then the Architect/Contract Administrator shall notify the Contractor of the same and give the Contractor 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 Contractor does not become compliant within the required time then the Architect/Contract Administrator has the right to obtain an independent audit against these standards in whole or in part.

3.5.5 If, as a result of any such independent audit as described in paragraph 1.5.4 the Contractor is found to be non-compliant with the principles and practices of ISO/IEC 27001 then the Contractor 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.

### 3.6 Breach of Security

3.6.1 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.

3.6.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 3.6.1, the Contractor shall:

3.6.2.1 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 Architect/Contract Administrator; and

3.6.2.2 as soon as reasonably practicable provide to the Architect/Contract Administrator 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

*[Guidance Note: Append Security Policy]*

### Appendix 2 – Security Management Plan

*[Guidance Note: Append Security Management Plan]*

**SCHEDULE** [Guidance: insert schedule ref here]

**CYBER ESSENTIALS**

**CYBER ESSENTIALS SCHEME**

**5. DEFINITIONS**

5.1 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.gov.uk/government/publications/cyber-essentials-scheme-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 Contractor 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 Contractor's cyber security approach under the Cyber Essentials Scheme and is a more advanced level of assurance.

**6. CYBER ESSENTIALS OBLIGATIONS**

2.1 Where the Employer's Requirements require that the Contractor provide a Cyber Essentials Certificate prior to the execution of the Works the Contractor shall provide a valid Cyber Essentials

Certificate, then on or prior to the commencement of the Works the Contractor delivers to the Employer evidence of the same. Where the Contractor fails to comply with this paragraph it shall be prohibited from commencing the carrying out of the works under any contract until such time as the Contractor has evidenced to the Employer its compliance with this paragraph 2.1.

2.2 Where the Contractor continues to Process Cyber Essentials Scheme Data during the carrying out of the works the Contractor shall deliver to the Employer evidence of renewal of the Cyber Essentials Certificate on each anniversary of the first applicable certificate obtained by the Contractor under paragraph 2.1.

2.3 Where the Contractor is due to Process Cyber Essentials Scheme Data after the commencement of the Works but before completion of the Works the Contractor shall deliver to the Employer evidence of:

2.3.1 a valid and current Cyber Essentials Certificate before the Contractor 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 Contractor under paragraph 2.1.

2.4 In the event that the Contractor 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 Contractor shall ensure that all sub-contracts with sub-contractors who Process Cyber Essentials Data contain provisions no less onerous on the sub-contractors than those imposed on the Contractor 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

## **SCHEDULE OF SPECIAL TERMS TO PPC2000 PROJECT PARTNERING CONTRACT (amended 2013) EDITION**

**Insert** new appendix:

### **"Appendix 12: Schedule of Amendments**

The Contract is modified by the Special Terms (which has been initialled on behalf of both parties) and is to be read and construed accordingly."

*[Preparation Note: Unless an electronic version of the PPC contract is being used AND this new Article has been inserted in the text of it as a Special Term, this new Article MUST be written, in manuscript, at the end of the Articles on the face of each PPC contract to be executed by the parties.]*

### **Clause 1.1. Definitions**

**Insert** the following new definitions:

"Commercially Sensitive Information: the information agreed between the parties (if any) comprising the information of a commercially sensitive nature relating to the Constructor, its IPR or its business or which the Constructor has indicated to the Client that, if disclosed by the Client, would cause the Constructor significant commercial disadvantage or material financial loss;

Confidential Information: the Client's Confidential Information and/or the Constructor's Confidential Information;

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

Constructor's Confidential Information: any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and contractors of the Constructor, 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;

Crown Body: any department, office or agency of the Crown

Data Controller: has the meaning given to it in the Data Protection Act 1998

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.

**Client Confidential Information:** all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and contractors of the Client, 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

**Client Data:**

- 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 Constructor by or on behalf of the Client; or
  - which the Constructor is required to generate, process, store or transmit pursuant to this Contract; or

any Personal Data for which the Client is the Data Controller to the extent that such Personal Data is held or processed by the Constructor.

**Environmental Information Regulations:** the Environmental Information Regulations 2004 and any guidance and/or codes of practice issued by the Information Commissioner 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 in relation to such legislation;

**General Anti-Abuse Rule:**

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

**Halifax Abuse Principle:** the principle explained in the CJEU Case C-255/02 Halifax and others

**Intellectual Property Rights" or "IPRs":**

(a) 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;

(b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and

(c) all other rights having equivalent or similar effect in any country or jurisdiction;

**Law:** 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 Constructor is bound to comply;

Occasion of Tax Non-Compliance:

- where any tax return of the Constructor 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 Constructor 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;
- The failure of an avoidance scheme which the Constructor was involved in, and which was, or should have been, notified to a Relevant Tax Authority under DOTAS or any equivalent or similar regime; and/or
- where any tax return of the Constructor 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.

Personal Data: the meaning given to it in the Data Protection Act 1998

Prohibited Act:

- to directly or indirectly offer, promise or give any person working for or engaged by the Client and/or the Authority or other Contracting Body or any other public body a financial or other advantage to:
  - induce that person to perform improperly a relevant function or activity; or
  - reward that person for improper performance of a relevant function or activity;
- to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this contract;
- committing any offence:
  - under the Bribery Act 2010 (or any legislation repealed or revoked by such Act)
  - under legislation or common law concerning fraudulent acts; or
  - defrauding, attempting to defraud or conspiring to defraud the Client; or
- any activity, practice or conduct which would constitute one of the offences listed above if such activity, practice or conduct had been carried out in the UK.

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 Information Regulations

Relevant Requirements: 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



Relevant Tax Authority: HM Revenue & Customs, or, if applicable, a tax authority in the jurisdiction in which the Constructor is established.

Security Policy: the Client's security policy attached as Appendix 1 to Schedule [Guidance: insert schedule ref here] (Security Policy) as may be updated from time to time"

### **1.6 Contracts (Rights of Third Parties) Act 1999**

1.6 In clause 1.6 After "clauses 7A and/or 7B" **insert** "and the express rights of any person under any collateral warranty granted under the provisions of this Contract,"

**Insert** new clauses 1.13 to 1.20 as follows:

#### **"MoD DEFCON Requirements**

1.13 The MoD special terms and conditions in the form of DEFCONs and DEFORMs shall be incorporated into this Contract as detailed in Contract Schedule [Guidance: insert schedule ref here]

#### **Freedom of information**

1.14.1 The Constructor acknowledges that unless the Client Representative has notified the Constructor that the Client is exempt from the provisions of the FOIA, the Client is subject to the requirements of the Code of Practice on Government Information, FOIA and the Environmental Information Regulations. The Constructor shall co-operate with and assist the Client so as to enable the Client to comply with its information disclosure obligations.

1.14.2 The Constructor shall:

1.14.2.1 transfer to the Client Representative 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;

1.14.2.2 provide the Client Representative with a copy of all Information in its possession, or power in the form that the Client Representative shall require within five Working Days (or such other period as the Client Representative may specify) of the Client Representative's request;

1.14.2.3 provide all necessary assistance as reasonably requested by the Client Representative to enable the Client to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations; and

1.14.2.4 procures that its sub-contractors do likewise.

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

1.14.4 The Constructor shall not respond directly to a Request for Information unless authorised to do so by the Client Representative.

1.14.5 The Constructor acknowledges that the Client 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 Constructor or despite the Constructor having expressed negative views when consulted.

1.14.6 The Constructor shall ensure that all Information is retained for disclosure for twelve years where this Contract is executed as a deed or six years where this Contract is executed under hand and shall permit the Client Representative to inspect such records as and when reasonably requested from time to time."

#### **1.15 Tax Compliance**

1.15.1 The Constructor represents and warrants that as at the date of this Contract, it has notified the Client in writing of any Occasions of Tax Non-Compliance or any litigation that it is involved in that is in connection with any Occasions of Tax Non-Compliance.

1.15.2 If, at any point prior to the end of the Rectification Period, an Occasion of Tax Non-Compliance occurs, the Constructor shall:

1.15.2.1 notify the Client in writing of such fact within 5 days of its occurrence; and

1.15.2.2 promptly provide to the Client:

1.15.2.2.1 details of the steps which the Constructor 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

1.15.2.2.2 such other information in relation to the Occasion of Tax Non-Compliance as the Client may reasonably require.

#### **1.16 GDPR**

The Client and the Constructor shall comply with the provisions of schedule [Guidance: insert schedule ref here]

#### **1.17 Confidentiality and Information Sharing**

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

1.17.1.1 treat the other party's Confidential Information as confidential and safeguard it accordingly; and

1.17.1.2 not disclose the other party's Confidential Information to any other person without the owner's prior written consent.

1.17.1.3 immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information

1.17.1.4 notify the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010

1.17.2 The clause above shall not apply to the extent that:

1.17.2.1 such disclosure is a requirement of the law of the contract placed upon the party making the disclosure, including any requirements for disclosure under the FOIA or the Environmental Information Regulations pursuant to clause 1.14 (Freedom of Information);

1.17.2.2 such information was in the possession of the party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;

1.17.2.3 such information was obtained from a third party without obligation of confidentiality;

1.17.2.4 such information was already in the public domain at the time of disclosure otherwise than by a breach of this Contract; or

1.17.2.5 it is independently developed without access to the other party's Confidential Information.

1.17.3 The Constructor may only disclose the Client's Confidential Information to Constructor's Persons who are directly involved in the provision of the service and who need to know the information, and shall ensure that such Constructor's Persons are aware of and shall comply with these obligations as to confidentiality.

1.17.4 The Constructor shall not, and shall procure that the Constructor's Persons do not, use any of the Client's Confidential Information received otherwise than for the purposes of this contract.

1.17.5 The Constructor may only disclose the Client's Confidential Information to Constructor's Persons who need to know the information, and shall ensure that such Constructor's Persons 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 Constructor's Persons causes or contributes (or could cause or contribute) to the Constructor breaching its obligations as to confidentiality under or in connection with this contract, the Constructor 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 Constructor Personnel, the Constructor shall provide such evidence to the Client as the Client may reasonably require (though not so as to risk compromising or prejudicing the case) to demonstrate that the Constructor is taking appropriate steps to comply with this clause, including copies of any written communications to and/or from Constructor's Persons, and any minutes of meetings and any other records which provide an audit trail of any discussions or exchanges with Constructor's Persons in connection with obligations as to confidentiality.

1.17.6 At the written request of the Client, the Constructor shall procure that those members of the Constructor's Persons identified in the Client's notice signs a confidentiality undertaking prior to commencing any work in accordance with this Contract.

1.17.7 Nothing in this Contract shall prevent the Client from disclosing the Constructor's Confidential Information:

1.17.7.1 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 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;

1.17.7.2 to any consultant, Constructor or other person engaged by the Client or any person conducting an Office of Government Commerce gateway review;

1.17.7.3 for the purpose of the examination and certification of the Client's accounts; or

1.17.7.4 for any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Client has used its resources.

and for the purposes of the foregoing, disclosure of the Constructor's Confidential Information shall be on a confidential basis and subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Client under this clause 1.17.

1.17.8 The Client shall use all reasonable endeavours to ensure that any government department, Contracting Body, employee, third party or sub-contractor to whom the Constructor's Confidential Information is disclosed pursuant to the above clause is made aware of the Client's obligations of confidentiality.

1.17.9 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

1.17.10 The Client may disclose the Confidential Information of the Constructor:

1.17.10.1 on a confidential basis to any Crown Body for any proper purpose of the Client or the relevant Crown Body;

1.17.10.2 to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;

1.17.10.3 to the extent that the Client (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;

1.17.10.4 on a confidential basis to a professional adviser, consultant, supplier or other person engaged by any Crown Body (including any benchmarking organisation) for any purpose connected with this Contract;

1.17.10.5 on a confidential basis for the purpose of the exercise of its rights under this Contract;

1.17.10.6 on a confidential basis to a proposed successor body of the Client in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under this Contract, and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Client under this clause.

## **1.18 Prevention of Fraud and Bribery**

1.18.1 The Constructor represents and warrants that neither it, nor to the best of its knowledge any of its employees, have at any time prior to the date of this Contract:

1.18.1.1 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

1.18.1.2 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.

1.18.2 During the carrying out of the Project the Constructor shall not:

1.18.2.1 commit a Prohibited Act; and/or

1.18.2.2 do or suffer anything to be done which would cause the Client or any of the Client's employees, consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements

1.18.3 During the carrying out of the Project the Constructor shall:

1.18.3.1 establish, maintain and enforce, and require that its sub-contractors 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;

1.18.3.2 keep appropriate records of its compliance with this Contract and make such records available to the Client on request;

1.18.3.3 provide and maintain and where appropriate enforce an anti-bribery policy (which shall be disclosed to the Client on request) to prevent it and any Constructor's employees or any person acting on the Constructor's behalf from committing a Prohibited Act.

1.18.4 The Constructor shall notify the Client immediately in writing if it becomes aware of any breach of clause 1.18.1, or has reason to believe that it has or any of the its employees or sub-contractors have:

1.18.4.1 been subject to an investigation or prosecution which relates to an alleged Prohibited Act;

1.18.4.2 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; and/or

1.18.4.3 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.

1.18.5 If the Constructor shall make a notification to the Client pursuant to clause 1.18.4, the Constructor shall respond promptly to the Client's enquiries, co-operate with any investigation, and allow the Client to audit any books, records and/or any other relevant documentation in accordance with this Contract.

1.18.6 If the Constructor breaches Clause 1.18.3, the Client may by notice require the Constructor to remove from carrying out the Project any Constructor's Person whose acts or omissions have caused the Constructor's breach.

### **1.19 Security requirements**

The Constructor shall comply with, and procure the compliance of the Constructor's Persons, with:

1.19.1 the Security Policy and the Security Management Plan and the Constructor shall ensure that the Security Management Plan produced by the Constructor fully complies with the Security Policy;

1.19.2 Contract Schedule [Guidance: insert schedule ref here] (Security Provisions).

### **1.20 Cyber Essentials**

The Client and the Constructor shall comply with the provisions of schedule [Guidance: insert schedule ref here] "

**Insert** new clauses 7.7A to 7.7B as follows

**"7.7A Admittance to the site**

7.7A.1 The Constructor shall submit details of people who are to be employed by it and its sub-contractors in connection with the Project to the Client Representative. The details shall include a list of names and addresses, the capabilities in which they are employed, and other information required by the Client Representative.

7.7A.2 The Client Representative may instruct the Constructor to take measures to prevent unauthorised persons being admitted to site. The instruction shall be valued as a Change if the measures are additional to those required by the Client's Requirements.

7.7A.3 Constructor's Persons are to carry a Client's pass and comply with all conduct requirements from the Client whilst they are on the parts of the site identified in the Client's Requirements.

7.7A.4 The Constructor shall submit to the Client Representative for acceptance a list of the names of the people for whom passes are required. The Client Representative shall issue the passes to the Constructor. Each pass shall be returned to the Client Representative when the employee no longer requires access to that part of the site or after the Client Representative has given notice that the employee is not to be admitted to the site.

7.7A.5 The Constructor shall not take photographs of the site or of work carried out in connection with the Project unless it has obtained the acceptance of the Client Representative.

7.7A.6 The Constructor shall take the measures needed to prevent any Constructor's Persons taking, publishing or otherwise circulating such photographs.

**7.7B Legislation and Official secrets**

7.7B.1 The Constructor shall comply with the Law in the carrying out of the Project.

7.7B.2 The Official Secrets Acts 1911 to 1989 and, where appropriate, the provisions of section 11 of the Atomic Energy Act 1946 apply to this Contract.

7.7B.3 The Constructor shall notify its employees and its sub-contractors of their duties under these Acts.

**Clause 9. Intellectual Property Rights**

**Amend** Appendix 1 – Definitions

**Delete** existing definition of Intellectual Property Rights and **add** in lieu

**"Intellectual Property Rights"** means any and all patents, trademarks, service marks, copyright, moral

rights, rights in a design, know-how, Confidential Information and all or any other intellectual or industrial property rights whether or not registered or capable of registration and whether subsisting in the United Kingdom or any other part of the world together with all or any goodwill relating or attached thereto;

**Add** new definitions

**“Confidential Information”** means any information designated as such by the Party disclosing that information; and

**“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 Constructor in relation to this Contract.

**Delete** existing clause 9 and **insert** the following:

“9.1 The Intellectual Property Rights in all Documents prepared by or on behalf of each Partnering Team member in relation to this Project Contract and the work executed from them remains the property of the relevant Partnering Team member. Each Partnering Team member hereby grants to the Client and the other Partnering Team members an irrevocable, royalty free, non-exclusive licence to use and reproduce the Documents for any and all purposes connected with the Partnering Contract. Such licence entitles the Client and each Partnering Team member to grant sub-licences to third parties in the same terms as this licence provided always that each Partnering Team member shall not be liable to any licensee for any use of the Documents or the Intellectual Property Rights in the Documents for purposes other than those for which the same were originally prepared by or on behalf of the Partnering Team member.

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

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

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

9.5 The Partnering Team member warrants to the Client that he has not granted and shall not (unless authorised by the Client) grant any rights to any third party to use or otherwise exploit the Documents.



9.6 The Partnering Team member shall supply copies of the Documents to the Client Representative and to the Client's other contractors and consultants for no additional fee to the extent necessary to enable them to discharge their respective functions in relation to this Contract or related works.

9.7 After the termination or conclusion of the Partnering Team member's employment hereunder, the Partnering Team member shall supply the Client Representative with copies and/or computer discs of such of the Documents as the Client Representative may from time to time request and the Client shall pay the Partnering Team member's reasonable costs for producing such copies or discs.

9.8 In carrying out the Project the Partnering Team member shall not infringe any Intellectual Property Rights of any third party. The Partnering Team member shall indemnify the Client against claims, proceedings, compensation and costs arising from an infringement or alleged infringement of the Intellectual Property Rights of any third party. "

## **Clause 10: Supply Chain**

**Insert** new clauses 10.15 to 10.16 as follows:

"10.15.1 a period for payment of the amount due to the Specialist not greater than 5 days after the final date for payment in this Partnering Contract. The amount due shall, but shall not be limited to, payment for work which the sub-contractor has completed from the previous application date up to the current application date in this Partnering Contract;

10.15.2 a provision requiring the Specialist to include in each subcontract 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 Partnering Contract; and

10.15.3 a provision requiring the Specialist to assess the amount due to a sub-contractor without taking into account the amount paid by the Constructor.

10.15.4 terms and conditions that are no less favourable than those of this Partnering Contract. The Client shall be entitled to reject Specialist conditions proposed by the Constructor that are unduly disadvantageous to the Specialist"

"10.16.1 The Constructor shall take all reasonable steps to engage SMEs as Specialists and to seek to ensure that no less than the percentage of the Specialists stated in the Client's Requirements (the "SME Percentage") are SMEs or that a similar proportion of the Agreed Maximum Price is undertaken by SMEs.

10.16.2 The Constructor shall report to the Client on a monthly basis the numbers of SMEs engaged as Specialists and the value of the Agreed Maximum Price that has been undertaken by SMEs.



10.16.3 Where available, the Constructor shall tender its Specialist contracts using the same online electronic portal as was provided by the Client for the purposes of tendering this Partnering Contract.”

## **Amend APPENDIX 9 - PROJECT BANK ACCOUNT**

**The following supplementary conditions shall be incorporated into Appendix 9 and shall prevail in the event of any inconsistency or conflict between the standard Appendix 9 conditions and these supplementary conditions.**

### **1. Definitions**

The following additional definitions shall apply to this Appendix:

Authorisation: a document authorising the Project Bank to make payments to the Constructor and Named Suppliers.

Named Suppliers: such Suppliers as are detailed in the Client's Requirements and such other Suppliers who have signed the Joining Deed.

Project Bank: the Bank as the Client shall inform the Constructor in writing

Project Bank Account: the Bank Account used to receive payments from the Client and to make payments to the Constructor and Named Suppliers

Trust Deed: an agreement in the form set out in this Appendix which contains provisions for administering the Project Bank Account.

Joining Deed: an agreement in the form set out in this Appendix under which the Specialist joins the Trust Deed.

### **2. Project Bank Account**

2.1 The Client shall establish the Project Bank Account with the Project Bank within three weeks of the date of this Partnering Contract.

2.2 Unless stated otherwise in the Client's Requirements, the Client shall pay any charges made and is paid any interest paid by the Project Bank. The charges and interest by the Project Bank are not included in the Agreed Maximum Price.

### **3. Named Suppliers**

The Constructor shall include in its contracts with Named Suppliers the arrangements in the contract for the operation of the Project Bank Account and Trust Deed. The Constructor shall inform the Named Suppliers of the details of the Project Bank Account and the arrangements for payment of amounts due under their contracts.

### **4. Payments**

4.1 The Constructor shall submit proposals for adding a Specialist to the Named Suppliers to the Client Representative for acceptance. A reason for not accepting is that the addition of such Specialist would not comply with the Client's Requirements. The Client, the Constructor and the Specialist shall sign the Joining Deed after acceptance

4.2 The Constructor shall show in the application for payment the amounts due to Named Suppliers in accordance with their contracts.

4.3 Within the time set out in the banking arrangements to allow the Project Bank to make payment to the Constructor and Named Suppliers in accordance with the Contract, the Client shall make payment to the Project Bank Account of the amount which is due to be paid under the Contract

4.4 The Constructor shall prepare the Authorisation, setting out the sums due to Named Suppliers as assessed by the Constructor and to the Constructor for the balance of the payment due under the Partnering Contract. After signing the Authorisation, the Constructor shall submit it to the Client Representative no later than four days before the final date for payment. The Client shall sign the Authorisation and submit it to the Project Bank no later than one day before the final date for payment.

4.5 The Constructor and Named Suppliers shall receive payment from the Project Bank Account of the sums set out in the Authorisation as soon as practicable after the Project Bank Account receives payment.

4.6 Any payment which is due from the Constructor to the Client shall not be made through the Project Bank Account

## **5. Effect of Payment**

Payments made from the Project Bank Account are treated as payments from the Client to the Constructor in accordance with the Contract or from the Constructor or Specialist to Named Supplier in accordance with their contracts as applicable. A delay in payment due to a failure of the Constructor to comply with the requirements of this clause is not treated as late payment under the Contract.

## **6. Trust Deed**

The Client, the Constructor and Named Suppliers shall sign the Trust Deed before the first Interim Valuation Date.

## **7. Termination**

If the Client Representative issues a termination certificate, no further payment is to be made into the Project Bank Account.

## FORM OF TRUST DEED

-----  
This agreement is made between the "**Client**", the "**Constructor**" and the Named Suppliers.

Terms in this deed have the meanings given to them in the contract between and for ("**Project**").

### BACKGROUND

The Client and the Constructor have entered into a contract for the Project.

The Named Suppliers have entered into contracts with the Constructor or a Specialist in connection with the Project.

The Constructor has established a Project Bank Account to make provision for payment to the Constructor and the Named Suppliers.

### AGREEMENT

The parties to this deed agree that:

11. sums due to the Constructor and Named Suppliers and set out in the Authorisation are held in trust in the Project Bank Account by the Constructor for distribution to the Constructor and Named Suppliers in accordance with the banking arrangements applicable to the Project Bank Account.
12. Further Named Suppliers may be added as parties to this deed with the agreement of the Client and Constructor. The agreement of the Client and Constructor is treated as agreement by the Named Suppliers who are parties to this deed.
13. This deed is subject to the law of the contract for the Project.
14. The benefits under this deed may not be assigned.

Executed as a deed, but not delivered until the )  
first date specified on page 1 by : )  
)

Signature

Name (block capitals)

Client

Signature

Name (block capitals)

*Standard 'boilerplate' amendments*

-----  
**Constructor**

-----  
Signature  
-----

-----  
Name (block capitals)  
-----

**Supplier**

## FORM OF JOINING DEED

This agreement is made between the "**Client**", the "**Constructor**" and ("**Additional Supplier**").

Terms in this deed have the meanings given to them in the contract between and for ("**Project**").

### BACKGROUND

The Client and the Constructor have entered into a contract for the Project.

The Named Suppliers have entered into contracts with the Constructor or a Specialist in connection with the Project.

The Constructor has established a Project Bank Account to make provision for payment to the Constructor and the Named Suppliers.

The Client, the Constructor and the Named Suppliers have entered into a deed as set out in Annex 1 ("**Trust Deed**"), and have agreed that the Additional Supplier may join that deed.

### AGREEMENT

The parties to this deed agree that:

15. The Additional Supplier becomes a party to the Trust Deed from the date set out below.
16. This deed is subject to the law of the contract for the Project.
17. The benefits under this deed may not be assigned.

Executed as a deed, but not delivered until the )  
first date specified on page 1 by : )  
)

Signature

Name (block capitals)

Client

Signature

Name (block capitals)

Constructor

*Standard 'boilerplate' amendments*

Signature

.....

Name (block capitals)

.....

**Additional Supplier**

**Amend** Appendix 10 (Building Information Modelling) as follows:

**Insert** the following clauses at the end of the Appendix:

12. A BIM Protocol applies/does not apply [delete as appropriate]
13. When a BIM Protocol applies it is detailed in the Employer's Information Requirements
14. When the CIC Building Information Modelling Protocol applies clauses 2.1.C.4 to 2.1.C.6.2 shall apply
15. In this clause, the Protocol is the CIC Building Information Modelling Protocol, first edition 2013. Terms used in this clause are those defined in the Protocol.
16. Clauses 1, 2, 5, 6, 7 of the Protocol shall form part of this Contract. Clauses 3 and 4 and Appendices 1 and 2 of the Protocol are deemed to be part of the Client's Requirements.
17. The following shall be deemed to be a Change:
  - 17.1. If the Constructor encounters an event which is outside his reasonable control and which prevents him from carrying out the work specified in clause 4.1.2 of the Protocol.
  - 17.2. If the Client revokes a licence granted under clause 6.6 of the Protocol.

**Insert** new appendix:

**"Appendix 13: Apprenticeships**

- 1 The Constructor shall take all reasonable steps to employ apprentices, and report to the Client the numbers of apprentices employed and the wider skills training provided, during the carrying out of the Project.
- 2 The Constructor shall take all reasonable steps to ensure that no less than the percentage of its employees stated in the Client's Requirements (the "Apprenticeship Percentage") are on formal apprenticeship programmes or that a similar proportion of hours worked in carrying out the Project, (which may include support staff and sub-contractors) are provided by employees on formal apprenticeship programmes.
- 3 The Constructor shall make available to its employees and Specialists working on the Partnering Contract, information about the Government's Apprenticeship programme and wider skills opportunities
- 4 The Constructor shall provide any further skills training opportunities that are appropriate for its employees engaged in carrying out the Project.
- 5 The Constructor shall provide a written report detailing the following measures in its regular contract management monthly reporting cycle and be prepared to discuss apprenticeships at its regular meetings with the Client Representative:
  - the number of people during the reporting period employed on the Partnering Contract, including support staff and Specialists;

- the number of apprentices and number of new starts on apprenticeships directly initiated through the procurement process;
- the percentage of all employees taking part in an apprenticeship programme;
- if applicable, an explanation from the Constructor as to why it is not managing to meet the specified percentage target;
- actions being taken to improve the take up of apprenticeships;
- other training/skills development being undertaken by employees 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."



**Insert** new appendix:

**"APPENDIX 14                      GDPR**

The following definitions shall apply to this Appendix 14

**Party** : a Party to this Agreement

**Agreement** : this contract;

**Law** : means any law, 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, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply;

**Processor Personnel** : means all directors, officers, employees, agents, consultants and Constructors 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, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [ subject to Royal Assent ] to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;

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

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

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)

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

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

Protective Measures: appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be

restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule [x] (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 Customer is the Controller and the Constructor is the Processor unless otherwise specified in Schedule

[X]. The only processing that the Processor is authorised to do is listed in Schedule [X] 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 [ X ], unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;
- (b) ensure that it has in place Protective Measures, are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:
  - (i) nature of the data to be protected;
  - (ii) harm that might result from a Data Loss Event;
  - (iii) state of technological development; and
  - (iv) cost of implementing any measures;
- (c) ensure that :
  - (i) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule X);

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

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

(B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

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

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

(d) not transfer Personal Data outside of the EU 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 (whether in accordance with GDPR Article 46 or LED Article 37) 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 [X] 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 [X] 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 [X] 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.

13. The contact details of the Controller's Data Protection Officer are: [Insert Contact details]
14. The contact details of the Processor's Data Protection Officer are: [Insert Contact details]
15. The Processor shall comply with any further written instructions with respect to processing by the Controller.
16. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	<p>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Constructor is the Processor in accordance with Clause 1.1.</p> <p>[Guidance: You may need to vary this section where (in the rare case) the Customer and Constructor have a different relationship. For example where the Parties are Joint Controller of some Personal Data:</p> <p>"Notwithstanding Clause 1.1 the Parties acknowledge that they are also Joint Controllers for the purposes of the Data Protection Legislation in respect of:</p> <p style="padding-left: 40px;">[Insert the scope of Personal Data which the purposes and means of the processing is determined by the both Parties]</p> <p>In respect of Personal Data under Joint Control, Clause 1.1-1.15 will not apply and the Parties agree to put in place a Joint Controller Agreement as outlined in Schedule Y instead."</p>

Subject matter of the processing	<p>[This should be a high level, short description of what the processing is about i.e. its subject matter of the contract.</p> <p>Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public. ]</p>
Duration of the processing	[Clearly set out the duration of the processing including dates]
Nature and purposes of the processing	<p>[Please be as specific as possible, but make sure that you cover all intended purposes.</p> <p>The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</p> <p>The purpose might include: employment processing, statutory obligation, recruitment assessment etc]</p>
Type of Personal Data being Processed	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]
Categories of Data Subject	[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]
<p>Plan for return and destruction of the data once the processing is complete</p> <p>UNLESS requirement under union or member state law to preserve that type of data</p>	[Describe how long the data will be retained for, how it be returned or destroyed]

**SCHEDULE** [Guidance: insert schedule ref here] **SECURITY PROVISIONS**

1. SECURITY PROVISIONS

1.1 Definitions

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

<b>"Affiliates"</b>	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;
<b>"Breach of Security"</b>	<p>in accordance with the Security Requirements and the Security Policy, the occurrence of:</p> <p>(g) any unauthorised access to or use of the Project, the Client Premises, the Sites, the Constructor System and/or any ICT, information or data (including the Confidential Information and the Client Data) used by the Client and/or the Constructor in connection with this Contract; and/or</p> <p>(h) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Client Data), including any copies of such information or data, used by the Client and/or the Constructor in connection with this Contract.</p>
<b>"Clearance"</b>	means national security clearance and employment checks undertaken by and/or obtained from the Defence Vetting Agency;
<b>"Commercially Sensitive Information"</b>	the information agreed between the parties (if any) [comprising the information of a commercially sensitive nature relating to the Constructor, its IPR or its business or which the Constructor has indicated to the Client that, if disclosed by the Client, would cause the Constructor significant commercial disadvantage or material financial loss];

***[Guidance Note: The Constructor's Commercially Sensitive Information should be agreed between the Client and the Constructor, together with the duration (if applicable) for which such information should remain confidential. This will assist the Client in respect of compliance with FOIA and the section 45 code published by the Department of Constitutional Affairs. If such information is listed in a specific document, please include the wording in square brackets in the above definition. If the***

*Standard 'boilerplate' amendments*

***information is not specifically listed in a specific document, please ensure that the above wording in square brackets in this definition is deleted.]***

<b>"Confidential Information"</b>	the Client's Confidential Information and/or the Constructor's Confidential Information;
<b>"Contracting Body"</b>	any Contracting Body as defined in Regulation 5(2) of the Public Contracts (Works, Service and Supply) (Amendment) Regulations 2000 other than the Client.
<b>"Constructor's Confidential Information"</b>	any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and Constructors of the Constructor, 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;
<b>"Constructor Equipment"</b>	the hardware, computer and telecoms devices and equipment supplied by the Constructor or its sub-contractors (but not hired, leased or loaned from the Client) for the carrying out of the Project;
<b>"Constructor Software"</b>	software which is proprietary to the Constructor, including software which is or will be used by the Constructor for the purposes of carrying out of the Project;
<b>"Constructor System"</b>	the information and communications technology system used by the Constructor in carrying out of the Project including the Software, the Constructor Equipment and related cabling (but excluding the Client System);
<b>"Control"</b>	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;
<b>"Crown Body"</b>	any department, office or agency of the Crown;
<b>"Default"</b>	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-contractors in connection with or in relation to the subject matter of this Contract and in respect of which such party



*Standard 'boilerplate' amendments*

	is liable to the other;
<b>"Dispute Resolution Procedure"</b>	the dispute resolution procedure set out in this Contract (if any) or as agreed between the parties;
<b>"Client Confidential Information"</b>	all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and Constructors of the Client, 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;
<b>"Client Premises"</b>	means premises owned, controlled or occupied by the Client or its Affiliates which are made available for use by the Constructor or its sub-contractors for carrying out of the Project (or any of them) on the terms set out in this Contract or any separate agreement or licence;
<b>"Client System"</b>	the Client's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Client or the Constructor in connection with this Contract which is owned by or licensed to the Client by a third party and which interfaces with the Constructor System or which is necessary for the Client to benefit from the Project;
<b>"Environmental Information Regulations"</b>	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;
<b>"FOIA"</b>	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;
<b>"Good Industry Practice"</b>	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;
<b>"ICT"</b>	information and communications technology;
<b>"ICT Environment"</b>	the Client System and the Constructor System;
<b>"Impact Assessment"</b>	an assessment of a Change Request;
<b>"Information"</b>	has the meaning given under section 84 of the Freedom of

## *Standard 'boilerplate' amendments*

Information Act 2000;

### **"Information Assets Register"**

the register of information assets to be created and maintained by the Constructor throughout the carrying out of the Project as described in the Contract (if any) or as otherwise agreed between the parties;

### **"Intellectual Property Rights" or "IPRs"**

(a) 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;

(b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and

(c) all other rights having equivalent or similar effect in any country or jurisdiction;

### **"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 Project;

### **"Know-How"**

all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the Project but excluding know how already in the Constructor's or the Client's possession before this contract;

### **"List x"**

means, in relation to a sub-contractor, one who has been placed on List x in accordance with Ministry of Defence guidelines and procedures, due to that sub-contractor 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

*Standard 'boilerplate' amendments*

Framework.

<b>"Regulatory Bodies"</b>	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 Client and "Regulatory Body" shall be construed accordingly;
<b>"Request for Information"</b>	a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations;
<b>"Security Management Plan"</b>	the Constructor's security plan prepared pursuant to paragraph 1.5.3 of this schedule (Security Management Plan) an outline of which is set out in Appendix 1 of this schedule (Security Management Plan);
<b>"Security Policy Framework"</b>	means the Cabinet Office Security Policy Framework (available from the Cabinet Office Security Policy Division);
<b>"Security Requirements"</b>	means the requirements in the Contract relating to security of the carrying out of the Project (if any) or such other requirements as the Client may notify to the Constructor from time to time
<b>"Security Tests"</b>	shall have the meaning set out in paragraph 2.4.1 of Part 2 of this Schedule (Security Management Plan);
<b>"Sites"</b>	any premises at which the Project are carried out or from which the Constructor manages, organises or otherwise directs the provision or the use of the Project or where any part of the Constructor System is situated or where any physical interface with the Client System takes place;
<b>"Software"</b>	Specially Written Software, Constructor Software and Third Party Software;
<b>"Specially Written Software"</b>	any software created by the Constructor (or by a third party on behalf of the Constructor) specifically for the purposes of this contract;
<b>"Staff Vetting Procedures"</b>	the Client'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;

*Standard 'boilerplate' amendments*

<b>"Statement of Applicability"</b>	shall have the meaning set out in ISO/IEC 27001 and as agreed by the parties during the procurement phase;
<b>"Standards"</b>	the British or international standards,[ Client'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;
<b>"Third Party Software"</b>	software which is proprietary to any third party other than an Affiliate of the Constructor which is or will be used by the Constructor for the purposes of carrying out of the Project; and

## 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 Project;
- 1.2.1.2 wider aspects of security relating to carrying out of the Project;
- 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 Constructor acknowledges that the Client places great emphasis on the confidentiality, integrity and availability of information and consequently on the security provided by the ISMS.
- 1.3.2 The Constructor 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;

*Standard 'boilerplate' amendments*

- 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 Client'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 Constructor gives an early warning to the Client Representative of such inconsistency immediately upon becoming aware of the same, and the Client Representative shall, as soon as practicable, advise the Constructor which provision the Constructor shall be required to comply with.
- 1.4 ISMS and Security Management Plan
- 1.4.1 Introduction:
    - 1.4.1.1 The Constructor shall develop, implement, operate, maintain and continuously improve and maintain an ISMS which will, without prejudice to paragraph 1.3.2, be approved, by the Client Representative, 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.
    - 1.4.1.2 The Constructor shall develop and maintain a Security Management Plan in accordance with this Schedule to apply during the carrying out of the Project.
    - 1.4.1.3 The Constructor shall comply with its obligations set out in the Security Management Plan.
    - 1.4.1.4 Both the ISMS and the Security Management Plan shall, unless otherwise specified by the Client, aim to protect all aspects of the Project and all processes associated with carrying out the Project, including the Affected Property, the Constructor System and any ICT,

information and data (including the Client Confidential Information and the Client Data) to the extent used by the Client or the Constructor 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 Constructor will prepare and deliver to the Client Representative for approval 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 Schedule.

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 approved by the Client Representative 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. If the Security Management Plan is not approved by the Client Representative the Constructor shall amend it within 10 Working Days or such other period as the parties may agree in writing of a notice of non-approval from the Client Representative and re-submit to the Client Representative for approval. The parties will use all reasonable endeavours to ensure that the approval 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 Client Representative. If the Client Representative does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Client Representative pursuant to this paragraph 1.4.2.2 of this schedule may be unreasonably withheld or delayed. However any failure to approve 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 Constructor in relation to all aspects of the Project and all processes associated with carrying out the Project and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Project 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

*Standard 'boilerplate' amendments*

responsibilities from those in place at the Contract Date to those incorporated in the Constructor's ISMS at the date notified by the Client Representative to the Constructor for the Constructor 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 Constructor and the Client engaged in the Project and shall only reference documents which are in the possession of the Client 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 Constructor annually or from time to time to reflect:

- (a) emerging changes in Good Industry Practice;
- (b) any change or proposed change to the Constructor System, the Project and/or associated processes;
- (c) any new perceived or changed security threats; and
- (d) any reasonable request by the Client Representative.

1.4.4.2 The Constructor will provide the Client Representative 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 Client. 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 Client Representative will approve any amendments or revisions to the ISMS or Security

*Standard 'boilerplate' amendments*

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 Constructor proposes to make to the ISMS or Security Management Plan (as a result of a Client Representative's request or change to the Project or otherwise) shall be subject to the early warning procedure and shall not be implemented until approved in writing by the Client Representative.

1.4.5 Testing

- 1.4.5.1 The Constructor shall conduct tests of the ISMS ("Security Tests") 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 Client Representative.

- 1.4.5.2 The Client Representative shall be entitled to witness the conduct of the Security Tests. The Constructor shall provide the Client Representative with the results of such tests (in a form approved by the Client 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 Client pursuant to this contract, the Client Representative and/or its authorised representatives shall be entitled, at any time and without giving notice to the Constructor, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Constructor's compliance with the ISMS and the Security Management Plan. The Client Representative may notify the Constructor 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 the Project. If such tests adversely affect the Constructor's ability to carry out the Project in accordance with the Client's Requirements, the Constructor 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 Constructor shall promptly notify the Client Representative of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Constructor proposes to make in order to correct such failure or weakness. Subject to the Client Representative's approval in accordance with paragraph 1.4.1.1, the Constructor shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the Client Representative or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS



*Standard 'boilerplate' amendments*

or Security Management Plan to address a non-compliance with the Security Policy or Security Requirements the change to the ISMS or Security Management Plan shall be at no cost to the Client.

1.5 Compliance with ISO/IEC 27001

- 1.5.1 Unless otherwise agreed by the parties, the Constructor shall obtain independent certification of the ISMS to ISO/IEC 27001 within 12 months of the Contract Date and shall maintain such certification for the duration of the contract.
- 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 Constructor reasonably believes that it is not compliant with ISO/IEC 27001, the Constructor shall promptly notify the Client Representative of this and the Client in its absolute discretion may waive the requirement for certification in respect of the relevant parts.
- 1.5.3 The Client Representative 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 Client Representative's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the Constructor, then the Client Representative shall notify the Constructor of the same and give the Constructor 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 Constructor does not become compliant within the required time then the Client Representative 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 Constructor is found to be non-compliant with the principles and practices of ISO/IEC 27001 then the Constructor 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 Client 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 Constructor shall:

*Standard 'boilerplate' amendments*

- 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 Client Representative; and
- 1.6.2.2 as soon as reasonably practicable provide to the Client Representative 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**

***[Guidance Note: Append Security Policy]***

**Appendix 2 – Security Management Plan**

***[Guidance Note: Append Security Management Plan]”***

Insert new appendix:

**"APPENDIX 15 - CYBER ESSENTIALS**

**CYBER ESSENTIALS SCHEME**

**1. DEFINITIONS**

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

<b>"Cyber Essentials Scheme"</b>	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: <a href="https://www.gov.uk/government/publications/cyber-essentials-scheme-overview">https://www.gov.uk/government/publications/cyber-essentials-scheme-overview</a> ;
<b>"Cyber Essentials Basic Certificate"</b>	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;
<b>"Cyber Essentials Certificate"</b>	Cyber Essentials Basic Certificate, the Cyber Essentials Plus Certificate or the Cyber Essential Scheme certificate equivalent to be provided by the Constructor as set out in the Framework Data Sheet;
<b>"Cyber Essential Scheme Data"</b>	sensitive and personal information and other relevant information as referred to in the Cyber Essentials Scheme; and
<b>"Cyber Essentials Plus Certificate"</b>	the certification awarded on the basis of external testing by an independent certification body of the Constructor'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 Client's Requirements require that the Constructor provide a Cyber Essentials Certificate prior to the execution of the Project the Constructor shall provide a valid Cyber Essentials Certificate, then on or prior to the commencement of the Project the Constructor delivers to the Client evidence of the same. Where the Constructor fails to comply with this paragraph it shall be prohibited from commencing the carrying out of the Project under any contract until such time as the Constructor has evidenced to the Client its compliance with this paragraph 2.1.

2.2 Where the Constructor continues to Process Cyber Essentials Scheme Data during the carrying out of the Project the Constructor shall deliver to the Client evidence of renewal of the Cyber Essentials Certificate on each anniversary of the first applicable certificate obtained by the Constructor under paragraph 2.1.

2.3 Where the Constructor is due to Process Cyber Essentials Scheme Data after the commencement of the Project but before completion of the Project the Constructor shall deliver to the Client evidence of:

2.3.1 a valid and current Cyber Essentials Certificate before the Constructor 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 Constructor under paragraph 2.1.

2.4 In the event that the Constructor fails to comply with paragraphs 2.2 or 2.3 (as applicable), the Client reserves the right to terminate this Contract for material Default.

2.5 The Constructor shall ensure that all sub-contracts with sub-contractors who Process Cyber Essentials Data contain provisions no less onerous on the sub-contractors than those imposed on the Constructor 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"