STANDARD ‘BOILERPLATE’ AMENDMENTS

NEC3 PSSC APRIL 2013

[ ] 2021

CABINET OFFICE

Crown Commercial Service

The standardised ‘boilerplate’ amendments project addresses a need to simplify the inclusion of government-specific clauses to the NEC, JCT and PPC2000 contracts. Centrally mandated government policies and some legislative requirements were being applied by a range of government departments, but as separate operations and with differing approaches. Scope was identified for a simple and standard set of terms which provide a unified front to implement policy and reduce the need for excessive additional drafting, creating a more efficient standardised approach. These terms would be applied across government construction contracts.

In order to bring about this situation, a cross-governmental review of construction contract amendments was undertaken by the Crown Commercial Service (CCS) and the Infrastructure and Projects Authority (IPA). Eighteen clauses were identified as those which would benefit most from the standardisation described above. These clauses were reviewed and redrafted to enhance their ease of comprehension, with the core wording translated to NEC, JCT and PPC2000 terminology.

These twenty four clauses are replicated within the NEC, JCT and PPC2000 boilerplate documents. This is the **NEC3 PSSC version.**

The clauses should be **unamended** save for those instances with an additional guidance note. Not all will be relevant to each project, and additional clauses may be required where not covered by this document. Those ‘boilerplate’ clauses not required can be removed and additional, project specific clauses may be added.

Process

The clauses are included in the contract by referring to them in the Contract Data Part 1 at Option Z. The template NEC3 PSSC Agreement Contract Data contains options to apply or disapply each of the Boilerplate Amendments. The following segment indicates the modification which must be made to the base contract, as well as the steps needed to incorporate the Boilerplate Amendments.

**NEC3 Professional Services Short Contract**

* In the Contract Data entry reading “the conditions of contract are the NEC4 Professional Services Short Contract (April 2013) and the following additional conditions” insert:

“The *additional conditions of contract* are as selected below and as detailed in the appended Standard Boilerplate Amendments.”

* Append pages 8 to 51 of this Standard ‘Boilerplate’ Amendments document to the standard contract document as this Schedule of Amendments.
* Confirm in the NEC3 template PSSC Agreement Contract Data which options apply or do not apply, or here not using the template PSSC Agreement Contract Data remove or strikethrough those clauses which do not apply to the current project .
* Add additional, project specific amendments in the normal way.

Table of Contents

# Summary of Clauses 4

**NEC 3** 9

Z2 Definitions 9

Z4 Admittance to Site 11

Z5 Prevention of Fraud and Bribery 12

Z6 Equality and Diversity………………………………………………………………………...13

Z7 Legislation and Official Secrets 14

Z8 Conflicts of interest………………………………………………………………………..….14

Z9 Publicity and Branding……………………………………………………………………..…14

Z10 Freedom of Information 15

Z13 Confidentiality and Information Sharing 15

Z14 Security Requirements 18

Z16 Tax Compliance 18

Z22 Fair Payment 18

Z26 Building Information Modelling (BIM) 19

Z44 Intellectual Property Rights 20

Z45 HMRC Requirements……………………………………………………………………….22

Z46 MOD DEFCONS 22

Z47 Small and Medium Enterprises (SMEs) 22

Z48 Apprenticeships 22

Z49 Change of Control……………………………………………………………………………24

Z50 Financial Standing……………………………………………………………………….…..24

Z51 Financial Distress…………………………………………………………………………....24

Z52 Records, audit access and open book data………………………………………………24

Z100 GDPR 26

Z101 Cyber Essentials 26

# Schedules

Financial Distress………………………………………………………………………………....27

GDPR 31

Security Provisions 38

Cyber Essentials 50

# SUMMARY OF CLAUSES

The following descriptions are of all the clauses addressed by the Standard ‘Boilerplate’ Amendments project. It should be noted that some of the clauses differ from document to document.

1. Definitions

A list of additional definitions must be included as an amendment to help explain the meaning of subsequent Boilerplate clauses.

1. Admittance to Site

This clause specifies additional provisions around how individual people may be admitted to the site, and the considerations which must be taken. This includes (but is not limited to) the provision of a list of employee names, obligations as to security passes, and the prevention of unauthorised access or taking of photographs.

1. Prevention of Fraud and Bribery

The Boilerplate clause expands the coverage of the standard contract Fraud and Bribery provisions. It introduces a ‘Prohibited Act’, also defined in the Boilerplate document, which must not be committed and which must be subject to suitable caution and management. The Consultant must hold subconsultants to the same standards, keep appropriate records of compliance, and immediately notify the Client of potential breaches and work with them to rectify the situation.

1. Equality and Diversity

This introduces an enforceable contractual obligation on the Consultant to comply with laws on equality and discrimination.

1. Official Secrets Act

Consultants are often required to abide by this Act due to the sensitive nature of some public sector projects. The Boilerplate clause saves Clients from drafting this themselves if required, creating an obligation to comply with this Act and, where appropriate, section 11 of the Atomic Energy Act 1946.

1. Conflicts of Interest

The Framework Agreement contains provisions for Consultants to avoid conflicts of interest and to notify them where they arise. This clause applies the same to the call-off contract and includes a right for the Client to terminate the contract if there is, or if the Client considers there to be, an actual conflict or a potential conflict of interest.

1. Publicity and Branding

Clients may not wish Consultants to publicise a project or make reference to a project in the Consultant’s promotional material. This clause prevents the Consultant from doing so without the Client’s consent.

1. Freedom of Information

As government departments are usually required to comply with Freedom of Information Act requests, extra clauses detailing how this obligation is to be respected must be included. The Boilerplate clause obliges the Consultant to work with the Client in satisfying these requests in certain ways. Among other considerations, this involves the retention and transferral of relevant information, communicating requests for information to the Client in a timely manner, and generally helping the Client in responding to the request.

1. Confidentiality and Information Sharing

Some public sector information is sensitive and cannot be shared, while at other times organisation must share details about its processes in the interest of transparency. As such, this clause provides obligations for both parties to safeguard confidential information, exceptions where that obligation does not apply, and additional restrictions on the Consultant and further rights for the Client.

1. Security Requirements

This clause is a preface to a schedule requiring the Consultant to create and maintain a comprehensive Information Security Management System. This must be agreed with the Client, contain measures sufficient to ensure security on the project in question, and be regularly reviewed to reflect changes in good practice or project details. It must be tested appropriately and be fully compliant with ISO 27001, subject to audits as required. The schedule also indicates some of the steps to be taken in the event of a security breach.

1. Tax Compliance

With the inclusion of this clause, the Consultant is under an obligation to notify the Client of relevant Tax Non Compliance. The Consultant must provide more information if the Occasion of Tax Non Compliance occurs prior to the defects date.

1. Fair Payment

This is a clause also aimed at improving how subconsultants are paid, similarly endorsed in the Government Construction Strategy 2016. Obligations are placed on the Consultant to assess and promptly pay subconsultants, and to ensure that these obligations are also included in their contracts with subconsultants.

1. Building Information Modelling (BIM)

Promoting and spreading the use of BIM techniques is a major government construction objective, as identified in the three main policy documents – the Government Construction Strategy 2016, Construction 2025, and the Construction Sector Deal. It has been mandated for all central government departments and is aimed at enhancing efficiency and reducing costs across the industry. This clause provides a mechanism for BIM Protocols to be applied as indicated in the Client’s Information Requirements. It is extracted from the NEC4 Professional Services Contract. NEC have issued notes on using the UK BIM Information Protocol (May 2020) with NEC Contracts.

1. Intellectual Property Rights

This indicates that the Consultant provides to the Client an irrevocable, royalty free and non- exclusive licence to use the Intellectual Property of the Consultant. The Client may transfer these rights in a variety of circumstances, and the Consultant is subject to a number of additional obligations.

1. HMRC Requirements

This provision is applicable only to HMRC projects and contracts. It incorporates their special terms and conditions.

1. MOD DEFCONs

This provision is applicable only to Ministry of Defence projects and contracts. It incorporates their special terms and conditions.

1. Small and Medium Enterprises (SMEs)

Government policy dictates that SMEs should be encouraged and brought into public sector projects, as reinforced in the Government Construction Strategy 2016, Construction Sector Deal and Construction 2025. There is a general target for 33% of central government procurement spend going to SMEs by 2022. This Boilerplate clause requires Consultants to employ a certain amount of SMEs as subconsultants, and to respect a number of other obligations regarding reporting and how they manage these SMEs.

1. Apprenticeships

In a similar way to SMEs, there is an overarching government policy for public sector organisations to promote the creation and use of apprenticeship schemes, as per the Government Construction Strategy 2016, the Construction Sector Deal and Construction 2025. In particular, a 2015 Procurement Policy Note describes the steps that public sector organisations must take to ensure they are meeting the government’s apprentice aims. This Boilerplate provides a way for Clients to ensure that Consultants do this by creating an obligation to employ certain amounts of apprentices. They must also provide further training opportunities and information about the Government Apprenticeship programme, and engage with the Client to review and discuss a number of measures relating to Apprenticeships.

1. Change of Control

The Framework Agreement contains provisions for alliance members to notify changes of control – for example through changes in voting rights, share capital or control of assets - where they arise. This clause applies the same to the call-off contract and includes a right for the Client to terminate the contract if there is a change of control.

1. Financial Standing

This clause replicates the clause in the Framework Agreement which allows for termination if there is a change in the Consultant’s financial standing which affects or may affect the Consultant’s ability to perform the contract.

1. Financial Distress

This clause is based in the schedule to the Framework Agreement and is a more detailed provision on changes to the Consultant’s credit rating, requiring the Consultant to provide a satisfactory continuity plan for approval. It also allows for termination if the Consultant fails to notify a significant downgrade in its credit rating, or fails to produce or comply with an approved continuity plan.

1. Records, audit access and open book data

This clause requires the Consultant to maintain full and accurate records and accounts of the operation of the contract including the service and the amounts paid by the Client. The Consultant is required to provide access to these records to any Client or other government auditor.

1. GDPR

With the advent of the General Data Protection Regulation (as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019), every construction project is required to include provisions within their contracts to ensure compliance. The Boilerplate document includes a Schedule so these regulations can be complied with, with areas for the parties to fill in to reflect project specific data protection requirements.

1. Cyber Essentials

This clause provides a way to include the Government Cyber Essentials scheme into construction projects. This scheme provides for a number of controls which organisations should implement to reduce the risk of common internet based threats. The clause lists obligations on the Consultant to provide proof of the required certification at certain stages of the project, and to apply the same obligations to its sub-consultants.

**SCHEDULE OF AMENDMENTS TO NEC3 PROFESSIONAL SERVICES SHORT CONTRACT**

# Option Z2 - Identified and defined terms

Insert new clause 11.3 additional defined terms.

11.3 (1) Auditor is:

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

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

11.3 (3) Client Confidential Information is all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and contractors of the Client, 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 (4) Client Data is the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and

• which are supplied to the *Consultant* by or on behalf of the *Client*,

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

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

11.3 (5) Client’s Premises are premises owned, occupied or leased by the *Client* and the site of any works to which the *services* relate.

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

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

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

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

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

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

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

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

11.3 (14) 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 (15) Environmental Information Regulations is the Environmental Information Regulations 2004 and any guidance and/or codes of practice issued by the Information Commissioner in relation to such regulations.

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

* 1. (17) General Anti-Abuse Rule is
     + the legislation in Part 5 of the Finance Act 2013 (as amended) and
     + any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements and to avoid national insurance contributions.

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

* 1. (19) Intellectual Property Rights or "IPRs" is
     + copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information,
     + applications for registration, and the right to apply for registration, for any of the rights listed in the first bullet point that are capable of being registered in any country or jurisdiction,
     + all other rights having equivalent or similar effect in any country or jurisdiction and
     + all or any goodwill relating or attached thereto.
  2. (20) Law is any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of

practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the *Consultant* is bound to comply under the *law of the contract*.

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

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

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

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

11.3 (23) Prohibited Act is

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

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

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

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

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

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

# Option Z4 - Admittance to Client’s Premises

Insert new clause 15:

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

15.2 The *Client* may instruct the *Consultant* to take measures to prevent unauthorised persons being admitted to the Client’s Premises.

15.3 All of the *Consultant*’s and subconsultant’s people are to carry an *Client’s* pass and comply with all conduct requirements from the *Client* whilst they are on the parts of the Client’s Premises identified in the Scope.

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

15.5 The *Consultant* does not take photographs of the Client’s Premises or of work carried out in connection with the *services* unless it has obtained the acceptance of the *Client*.

15.6 The *Consultant* takes the measures needed to prevent its and its subconsultants’ people taking, publishing or otherwise circulating such photographs.

# Option Z5 - Prevention of fraud and bribery

Insert new clauses:

16.1 The *Consultant* represents and warrants that neither it, nor to the best of its knowledge any of its people, have at any time prior to the date of this contract

* + - * 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.

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

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

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

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

16.4 The *Consultant* immediately notifies the *Client* in writing if it becomes aware of any breach of clause 16.1, or has reason to believe that it has or any of its employees or subconsultants have

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

16.5 If the *Consultant* makes a notification to the *Client* pursuant to clause 16.4, the *Consultant* responds promptly to the *Client's* enquiries, co-operates with any investigation, and allows the *Client* to audit any books, records and/or any other relevant documentation in accordance with this contract.

16.6 If the *Consultant* breaches Clause 16.3, the *Client* may by notice require the *Consultant* to remove from carrying out the *services* any *Consultant* employee whose acts or omissions have caused the *Consultant*’s breach.

**Option Z6 - Equality and diversity**

Insert new clauses:

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

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

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

# Option Z7 - Legislation and Official secrets

Insert new clauses:

21.4 The *Consultant* complies with Law in the carrying out of the *services.*

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

21.6 The *Consultant* notifies its people and its subconsultants of their duties under these Acts.

# Option Z8 – Conflicts of interest

# Insert new clauses:

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

# 27.2. The *Consultant* promptly notifies and provides full particulars to the Client if such conflict referred to in clause 27.1 arises or may reasonably been foreseen as arising.

# 27.3. The *Client* may terminate the *Consultant’s* obligation to Provide the Services immediately under the second bullet point of clause 90.2 and/or to take such other steps the *Client* deems necessary where, in the reasonable opinion of the *Client*, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the *Consultant* and the duties owed to the *Client* under this contract.

# Option Z9 – Publicity and Branding

# Insert new clauses:

28.1 The *Consultant* does not

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

without approval of the *Client*.

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

# Option Z10 - Freedom of information

Insert new clauses:

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

23.2 The *Consultant*

* transfers to the *Client* 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 *Client* with a copy of all information in its possession, or power in the form that the *Client* requires within five working days (or such other period as the *Client* may specify) of the *Client’s* request,
* provides all necessary assistance as reasonably requested by the *Client* 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 subconsultants do likewise.

23.3 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.

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

23.5 The *Consultant* 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 *Consultant* or despite the *Consultant* having expressed negative views when consulted.

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

# Option Z13 - Confidentiality and Information Sharing

Insert a new clause

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

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

24.2 The clause above shall not apply to the extent that

* such disclosure is a requirement of the Law placed upon the Party making the disclosure, including any requirements for disclosure under the FOIA or the Environmental Information Regulations pursuant to clause Z10 (Freedom of Information),
* such information was in the possession of the Party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner,
* such information was obtained from a third party without obligation of confidentiality,
* such information was already in the public domain at the time of disclosure otherwise than by a breach of this contract or
* it is independently developed without access to the other Party's Confidential Information.

24.3 The *Consultant* may only disclose the ClientConfidential Information to the people who are directly involved in the carrying out of the *services* and who need to know the information, and shall ensure that such people are aware of and shall comply with these obligations as to confidentiality.

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

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

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

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

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

and for the purposes of the foregoing, disclosure of the Consultant’s Confidential Information shall be on a confidential basis and subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the *Client* under this clause 24.6.

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

24.8 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.

24.9 The *Client* may disclose the Consultant’s Confidential Information

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

# Option Z14 - Security Requirements

The *Consultant* complies with, and procures the compliance of the *Consultant’*s people, with the Security Policy and the Security Management Plan produced by the *Consultant* and the *Consultant* shall ensure that the Security Management Plan fully complies with the Security Policy and Contract Schedule [[Guidance: insert schedule ref here].

# Option Z16 - Tax Compliance

Insert new clauses:

25.1 The *Consultant* represents and warrants that 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.

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

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

# Option Z22 - Fair payment

Insert a new clause:

53.1 The *Consultant* assesses the amount due to a subconsultant without taking into account the amount certified by the *Client*.

53.2 The *Consultant* includes in the contract with each subconsultant

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

# Option Z26 - Building Information Modelling (BIM)

Insert a new clause:

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

21.A.2 If a BIM Protocol applies the following is added to the Contract Data

the *information execution plan* is ……………………

21A.3 In this clause 21A the following defined terms apply:

**The Information Execution Plan** is the *information execution plan* or is the latest Information Execution Plan accepted by the *Client*. The latest Information Execution Plan accepted by the *Client* supersedes the previous Information Execution Plan.

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

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

**The Information Model Requirements** are the requirements identified in the Scope for creating or changing the Information Model.

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

21A.4 The *Consultant* collaborates with other Information Providers as stated in the Information Model Requirements.

21A.5 The *Consultant* and the *Client* give an early warning by notifying the other as soon as either becomes aware of any matter which could adversely affect the creation or use of the Information Model.

21A.6 If an Information Execution Plan is not identified in the date of this contract, the *Consultant* submits a first Information Execution Plan to the *Client* for acceptance within the period stated in the Contract Data.

21A.7 Within two weeks of the *Consultant* submitting an Information Execution Plan for acceptance, the *Client* notifies the *consultant* of the acceptance of the Information Execution Plan or the reasons for not accepting it. A reason for not accepting in Information Execution Plan is that

● it does not comply with the Information Model Requirements or

● it does not allow the *Consultant* to Provide the Services.

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

21A.8 The *Consultant* submits a revised Information Execution Plan to the *Client* for acceptance

● within the *period for reply* after the *Client* has instructed it to and

● when the *Consultant* chooses to.

21A.9 The *Consultant* provides the Project Information in the form stated in the Information Model Requirements and in accordance with the accepted Information Execution Plan.

21A.10 If the Information Execution Plan is altered by a compensation event, the *Consultant* includes the alterations to the Information Execution Plan in the quotation for the compensation event.

21A.11 The *Client* owns the Information Model and the *Consultant’s* rights over Project Information except as stated otherwise in the Information Model Requirements. The *Consultant* obtains from a subconsultant equivalent rights for the *Client* over information prepared by the subconsultant. The *Consultant* provides to the *Client* the documents which transfer these rights to the *Client*.

21A.12 The following are *Client’s* risks

● A fault or error in the Information Model other than a Defect in the Project Information.

● A fault in information provided by Information Providers other than the *Consultant*.

21A.13 The *Consultant* is not liable for a fault or error in the Project Information unless it failed to provide the Project Information using the skill and care normally used by professionals providing information similar to the Project Information.

**Option Z44 - Intellectual Property Rights** Delete clause 70 and insert the following clause In this clause 70 only:

**“Document”** means all designs, drawings, specifications, software, electronic data,

photographs, plans, surveys, reports, and all other documents and/or information prepared by or on behalf of the *Consultant* in relation to this contract.

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

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

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

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

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

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

70.7 The *Consultant* supplies copies of the Documents to the *Client* 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 services.

70.8 After the termination or conclusion of the *Consultant*’s employment hereunder, the *Consultant* supplies the *Client* with copies and/or computer discs of such of the Documents as the *Client* may from time to time request and the *Client* pays the *Consultant*’s reasonable costs for producing such copies or discs.

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

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

# Option Z45 – HMRC Requirements

Insert a new clause 17

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

# Option Z46 - MoD DEFCON Requirements

Insert a new clause 17

This clause is to incorporate MoD special terms and conditions in the form of DEFCONs and DEFORMs as detailed at [https://www.gov.uk/guidance/knowledge-in-defence-kid](https://protect-eu.mimecast.com/s/NShMCNxBzcXyxEVcmva1a?domain=gov.uk)

# Option Z47 - Small and Medium Sized Enterprises (SMEs)

Insert new clause:

22.4

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

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

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

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

# Option Z48 - Apprenticeships

Insert new clause:

22.5

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

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

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

The *Consultant* provides any further skills training opportunities that are appropriate for its people engaged in carrying out the *services*.

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

* the number of people during the reporting period employed on the contract, including support staff and subconsultants,
* the number of apprentices and number of new starts on apprenticeships directly initiated through this contract,
* the percentage of all people taking part in an apprenticeship programme,
* if applicable, an explanation from the *Consultant* as to why it is not managing to meet the specified percentage target,
* actions being taken to improve the take up of apprenticeships and
* other training/skills development being undertaken by people in relation to this contract, including:
  + 1. work experience placements for 14 to 16 year olds,
    2. work experience /work trial placements for other ages,
    3. student sandwich/gap year placements,
    4. graduate placements,
    5. vocational training,
    6. basic skills training and
    7. on site training provision/ facilities.

# Option Z49 – Change of Control

Insert new clauses:

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

90.4 The *Client* may terminate the *Consultant’s* obligation to Provide the Services (which shall take effect as termination under the second bullet point of clause 90.2) within six months from

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

# Option Z50 – Financial Standing

90.5 The *Client* may terminate the *Consultant’s* obligation to Provide the Services (which shall take effect as termination under the second bullet point of clause 90.2) where in the reasonable opinion of the *Client* there is a material detrimental change in the financial standing and/or the credit rating of the *Consultant* which:

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

# Option Z51 – Financial Distress

The *Consultant* complies with the provisions of Schedule [Guidance: insert schedule ref here] (Financial Distress) in relation to the assessment of the financial standing of the *Consultant* and the consequences of a change to that financial standing.

# Option Z52 – Records, audit access and open book data

Insert new clauses:

29.1 The *Consultant* keeps and maintains for theperiodof the *Consultant’s* liability under this contract full and accurate records and accounts of the operation of this contract including the *service* provided under it, any subcontracts and the amounts paid by the *Client*.

29.2 The Consultant

* keeps the records and accounts referred to in clause 29.1 in accordance with Law
* affords any Auditor access to the records and accounts referred to in clause 29.1 at the *Consultant’s* premises and/or provides records and accounts (including copies of the *Consultant’s* published accounts) or copies of the same, as may be required by any Auditor from time to time during the *Consultant* Providing the Services and the liability period under the contract in order that the Auditor may carry out an inspection to assess compliance by the *Consultant* and/or its subconsultants of any of the *Consultant’s* obligations under this contract including in order to:
* verify the accuracy of any amounts payable by the *Client* under this contract (and proposed or actual variations to them in accordance with this contract)
* verify the costs of the *Consultant* (including the costs of all subconsultants and any third party suppliers) in connection with Providing the Services
* identify or investigate an actual or suspected Prohibited Act, impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the *Client* has no obligation to inform the *Consultant* of the purpose or objective of its investigations
* obtain such information as is necessary to fulfil the *Client’s* obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General
* enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the *Client* has used its resources
* subject to the *Consultant’s* rights in respect of Consultant’s Confidential Information, the *Consultant* provides the Auditor on demand with all reasonable co-operation and assistance in respect of
* all reasonable information requested by the *Client* within the scope of the audit
* reasonable access to sites controlled by the *Consultant* and to any *Consultant’s* equipment used to Provide the Service
* access to the *Consultant’s* personnel.

29.3 The Parties bear their own respective costs and expenses incurred in respect of compliance with their obligations under this clause 29, unless the audit reveals a default by the *Consultant* in which case the *Consultant* reimburses the *Client* for the *Client’s* reasonable costs incurred in relation to the audit.

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

# Option Z100 – GDPR

Insert new clause Z100 as follows:

# Z100 GDPR

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

# Option Z101 – Cyber Essentials

Insert new clause Z101 as follows:

# Z101 Cyber Essentials

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

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

**1. Definitions**

1.1. In this Schedule [ ] the following definitions apply:

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

“Financial Distress Event” means the occurrence or one or more of the events listed in this Schedule [ ]

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

"Rating Agency" means the rating agency means Dun & Bradstreet.

**2. Credit rating and duty to notify**

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

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

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

Where

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

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

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

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

2.4. The *Consultant*:

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

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

**3. Consequences of a financial distress event**

3.1. In the event of:

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

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

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

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

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

3.1.6. any of the following:

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

then, immediately upon notification of the Financial Distress Event (or if the *Client* becomes aware of the Financial Distress Event without notification and brings the event to the attention of the *Consultant*), the *Consultant* shall have the obligations and the *Client* shall have the rights and remedies as set out in paragraphs 3.2 – 3.6.

3.2. The *Consultant*:

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

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

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

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

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

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

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

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

**4. Termination rights**

4.1. The *Client* may terminate the *Consultant’s* obligation to Provide the Service (which shall take effect as termination under the second bullet point of clause 90.2) if

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

**5. Primacy of credit ratings**

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

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

**ANNEX 1: CREDIT RATINGS & CREDIT RATING THRESHOLDS**

*Consultant* Credit current rating (long term) [ ]

Credit Rating Threshold [ ]

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

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

**Agreement** : this contract;

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

# GDPR CLAUSE DEFINITIONS:

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

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

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

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

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

DPA 2018 : Data Protection Act 2018

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

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

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

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

# DATA PROTECTION

* 1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the *Client* is the Controller and the *Consultant* is the Processor unless otherwise specified in Schedule [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.
  2. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
  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:

1. a systematic description of the envisaged processing operations and the purpose of the processing;
2. an assessment of the necessity and proportionality of the processing operations in relation to the *services*;
3. an assessment of the risks to the rights and freedoms of Data Subjects; and
4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
   1. The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:
5. 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;
6. 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:
7. nature of the data to be protected;
8. harm that might result from a Data Loss Event;
9. state of technological development; and
10. cost of implementing any measures;
11. ensure that :
12. the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule X);
13. 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:
14. are aware of and comply with the Processor’s duties under this clause;
15. are subject to appropriate confidentiality undertakings with the Processor or any Sub- processor;
16. 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
17. have undergone adequate training in the use, care, protection and handling of Personal Data; and
18. not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
19. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (the Data Protection Legislation) as determined by the Controller;
20. the Data Subject has enforceable rights and effective legal remedies;
21. 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
22. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
23. 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. Subject to clause 1.6, the Processor shall notify the Controller immediately if it:
24. receives a Data Subject Request (or purported Data Subject Request);
25. receives a request to rectify, block or erase any Personal Data;
26. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
27. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
28. 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
29. becomes aware of a Data Loss Event.
    1. 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.
    2. 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:
30. the Controller with full details and copies of the complaint, communication or request;
31. 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;
32. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
33. assistance as requested by the Controller following any Data Loss Event;
34. 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. 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:
35. the Controller determines that the processing is not occasional;
36. 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
37. the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
    1. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller’s designated auditor.
    2. Each Party shall designate its own data protection officer if required by the Data Protection Legislation .
    3. Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:
38. notify the Controller in writing of the intended Sub-processor and processing;
39. obtain the written consent of the Controller;
40. 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
41. provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.
    1. The Processor shall remain fully liable for all acts or omissions of any of its Sub- processors.
    2. 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).
    3. 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.
    4. 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 | The Parties acknowledge that for the purposes of the Data Protection Legislation, the *Client* is the Controller and the *Consultant* is the Processor in accordance with Clause 1.1.  [Guidance: You may need to vary this section where (in the rare case) the *Client* and *Consultant* have a different relationship. For example where the Parties are Joint Controller of some Personal Data:  “Notwithstanding Clause 1.1 the Parties acknowledge that they are also Joint Controllers for the purposes of the Data Protection Legislation in respect of:  [Insert the scope of Personal Data which the purposes and means of the processing is determined by the both Parties]  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.” |
| Subject matter of the processing | [This should be a high level, short description of what the processing is about i.e. its subject matter of the contract.  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. ] |
| Duration of the processing | [Clearly set out the duration of the processing including dates] |
| Nature and purposes of the processing | [Please be as specific as possible, but make sure that you cover all intended purposes.  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. |

|  |  |
| --- | --- |
|  | 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 | [Describe how long the data will be retained for, how it be returned or destroyed] |
| UNLESS requirement under union or member state law to preserve that type of  data |  |

# SCHEDULE [Guidance: insert schedule ref here]

1. CONTRACT SCHEDULE [Guidance: insert schedule ref here] - SECURITY PROVISIONS
   1. Definitions

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

**"Affiliates"** in relation to a body corporate, any other entity which

directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;

**"Breach of Security"** in accordance with the Security Requirements and the

Security Policy, the occurrence of:

* + 1. any unauthorised access to or use of the services the Client Premises, the Sites, the Consultant System and/or any ICT, information or data (including the Confidential Information and the Client Data) used by the *Client* and/or the *Consultant* in connection with this contract; and/or
    2. 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 *Consultant* in connection with this contract.

**"Clearance"** means national security clearance and employment checks

undertaken by and/or obtained from the Defence Vetting Agency;

# "Consultant Equipment"

the hardware, computer and telecoms devices and equipment supplied by the *Consultant* or its Subconsultants (but not hired, leased or loaned from the *Client*) for the carrying out of the *services*;

**"Consultant Software"** software which is proprietary to the *Consultant*, including

software which is or will be used by the *Consultant* for the purposes of carrying out of the *services*;

**"Consultant System"** the information and communications technology system

used by the *Consultant* in carrying out of the *services* including the Software, the Consultant Equipment and related cabling (but excluding the Client System);

**"Control"** means that a person possesses, directly or indirectly, the

power to direct or cause the direction of the management

and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "Controls" and "Controlled" shall be interpreted accordingly;

**"Default"** any breach of the obligations of the relevant party (including but not limited to fundamental breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant party, its employees, servants, agents or Sub Consultants in connection with or in relation to the subject-matter of this contract and in respect of which such party is liable to the other;

# "Dispute Resolution Procedure"

the dispute resolution procedure set out in this contract (if any) or as agreed between the parties;

**"Client Premises"** means premises owned, controlled or occupied by the

*Client* or its Affiliates which are made available for use by the *Consultant* or its Subconsultants for carrying out of the *services* (or any of them) on the terms set out in this contract or any separate agreement or licence;

**"Client System"** the *Client*'s computing environment (consisting of

hardware, software and/or telecommunications networks or equipment) used by the *Client* or the *Consultant* in connection with this contract which is owned by or licensed to the *Client* by a third party and which interfaces with the Consultant System or which is necessary for the *Client* to receive the *services*;

# "Environmental Information Regulations"

the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issues by the Information Commissioner or relevant Government Department in relation to such regulations;

**"FOIA"** the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such legislation;

# "Good Industry Practice"

the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector;

**"ICT"** information and communications technology;

**"ICT Environment"** the Client System and the Consultant System;

**"Impact Assessment"** an assessment of a Compensation Event;

**"Information"** has the meaning given under section 84 of the Freedom of

Information Act 2000;

# "Information Assets Register"

the register of information assets to be created and maintained by the *Consultant* throughout the carrying out of the *services* as described in the contract (if any) or as otherwise agreed between the parties;

**"ISMS"** the Information Security Management System as defined by ISO/IEC 27001. The scope of the ISMS will be as agreed by the parties and will directly reflect the scope of the *services*;

**"Know-How"** all ideas, concepts, schemes, information, knowledge,

techniques, methodology, and anything else in the nature of know how relating to the *services* but excluding know how already in the *Consultant*’s or the *Client*’s possession before this contract;

**"List x"** means, in relation to a Subconsultant, one who has been placed on List x in accordance with Ministry of Defence guidelines and procedures, due to that Sub Consultant undertaking work on its premises marked as CONFIDENTIAL or above;

**"Malicious Software"** any software program or code intended to destroy, interfere

with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;

**"Process"** has the meaning given to it under the Data Protection

Legislation but, for the purposes of this contract, it shall include both manual and automatic processing;

**"Protectively Marked"** shall have the meaning as set out in the Security Policy

Framework.

**"Regulatory Bodies"** those government departments and regulatory, statutory

and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this contract or any other affairs of the *Client* and "Regulatory Body" shall be construed accordingly;

# "Request for Information"a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations;

# "Security Management Plan"

**"Security Policy Framework"**

**"Security Requirements"**

the *Consultant*'s 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);

means the Cabinet Office Security Policy Framework (available from the Cabinet Office Security Policy Division);

means the requirements in the contract relating to security of the carrying out of the *services* (if any) or such other

requirements as the *Client* may notify to the *Consultant* from time to time

**"Security Tests"** shall have the meaning set out in Appendix 2 (Security

Management Plan) [Guidance: define “Security Tests” in Security Management Plan]

**"Software"** Specially Written Software, *Consultant* Software and Third

Party Software;

# "Specially Written Software"

**"Staff Vetting Procedures"**

**"Statement of Applicability"**

any software created by the *Consultant* (or by a third party on behalf of the *Consultant*) specifically for the purposes of this contract;

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;

shall have the meaning set out in ISO/IEC 27001 and as agreed by the parties during the procurement phase;

**"Standards"** the British or international standards, *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;

**"Third Party Software"** software which is proprietary to any third party other than

an Affiliate of the *Consultant* which is or will be used by the

*Consultant* for the purposes of carrying out of the *services.*

* 1. Introduction
     1. This schedule covers:
        1. principles of protective security to be applied in carrying out of the *services*;
        2. wider aspects of security relating to carrying out of the *services*;
        3. the development, implementation, operation, maintenance and continual improvement of an ISMS;
        4. the creation and maintenance of the Security Management Plan;
        5. audit and testing of ISMS compliance with the Security Requirements;
        6. conformance to ISO/IEC 27001 (Information Security Requirements Specification) and ISO/IEC27002 (Information Security Code of Practice) and;
        7. obligations in the event of actual, potential or attempted breaches of security.
  2. Principles of Security
     1. The *Consultant* acknowledges that the *Client* places great emphasis on the confidentiality, integrity and availability of information and consequently on the security provided by the ISMS.
     2. The *Consultant* shall be responsible for the effective performance of the ISMS and shall at all times provide a level of security which:
        1. is in accordance with Good Industry Practice, the *law of the contract* and this contract;
        2. complies with the Security Policy;
        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);
        4. meets any specific security threats to the ISMS; and
        5. complies with ISO/IEC27001 and ISO/IEC27002 in accordance with paragraph [1.3.2](#bookmark1) of this schedule;
        6. complies with the Security Requirements; and
        7. complies with the *Client*’s ICT standards.
     3. The references to standards, guidance and policies set out in paragraph

[1.3.2.2](#bookmark2) 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. In the event of any inconsistency in the provisions of the above standards, guidance and policies, the *Consultant* gives an early warning to the *Client* of such inconsistency immediately upon becoming aware of the same, and the *Client* shall, as soon as practicable, advise the *Consultant* which provision the *Consultant* shall be required to comply with.
  1. ISMS and Security Management Plan
     1. Introduction:
        1. The *Consultant* shall develop, implement, operate, maintain and continuously improve and maintain an ISMS which will, without prejudice to paragraph [1.3.2](#bookmark1), be accepted, by the *Client*, 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. The *Consultant* shall develop and maintain a Security Management Plan in accordance with this Schedule to apply during the carrying out of the *services*.
        3. The *Consultant* shall comply with its obligations set out in the Security Management Plan.
        4. Both the ISMS and the Security Management Plan shall, unless otherwise specified by the *Client*, aim to protect all aspects of the *services* and all processes associated with carrying out of the *services*, including the construction, use, alterations or demolition of the *services*, the Consultant System and any ICT, information and data (including the Client Confidential Information and the Client Data) to the extent used by the *Client* or the *Consultant* in connection with this contract.
     2. Development of the Security Management Plan:
        1. Within 20 Working Days after the date of this contract and in accordance with paragraph [1.4.4](#bookmark6) (Amendment and Revision), the *Consultant* will prepare and deliver to the *Client* for acceptance a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan set out in Appendix 2 of this Part 2 of this Contract Schedule J.
        2. If the Security Management Plan, or any subsequent revision to it in accordance with paragraph [1.4.4](#bookmark6) (Amendment and Revision), is accepted by the *Client* it will be adopted immediately and will replace the previous version of the Security Management Plan at Appendix 2 of this Part 2 of this Contract Schedule J. If the Security Management Plan is not accepted by the *Client* the *Consultant* shall amend it within 10 Working Days or such other period as the parties may agree in writing of a notice of non-acceptance from the *Client* and re-submit to the *Client* for acceptance. The parties will use all reasonable endeavours to ensure that the acceptance process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the parties may agree in writing) from the date of its first submission to the *Client*. If the *Client* does not accept the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. No acceptance to be given by the *Client* pursuant to this paragraph [1.4.2.2](#bookmark4) of this schedule may be unreasonably withheld or delayed. However any failure to accept the Security Management Plan on the grounds that it does not comply with the requirements set out in paragraph [1.4.3.4](#bookmark5) shall be deemed to be reasonable.
     3. Content of the Security Management Plan:
        1. The Security Management Plan will set out the security measures to be implemented and maintained by the *Consultant* in relation to all aspects of the *services* and all processes associated with carrying out of the *services* and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the *services* comply with the provisions of this schedule (including the principles set out in paragraph [1.3](#bookmark0));
        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 date of this contract to those incorporated in the *Consultant*’s ISMS at the date notified by the *Client* to the *Consultant* for the *Consultant* to meet the full obligations of the Security Requirements.
        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.
        4. The Security Management Plan shall be written in plain English in language which is readily comprehensible to the staff of the *Consultant* and the *Client* engaged in the *services* and shall only reference documents which are in the possession of the *Client* or whose location is otherwise specified in this schedule.
     4. Amendment and Revision of the ISMS and Security Management Plan:
        1. The ISMS and Security Management Plan will be fully reviewed and updated by the *Consultant* annually or from time to time to reflect:
           1. emerging changes in Good Industry Practice;
           2. any change or proposed change to the Consultant System, the *services* and/or associated processes;
           3. any new perceived or changed security threats; and
           4. any reasonable request by the *Client*.
        2. The *Consultant* will provide the *Client* 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:
           1. suggested improvements to the effectiveness of the ISMS;
           2. updates to the risk assessments;
           3. proposed modifications to the procedures and controls that effect information security to respond to events that may impact on the ISMS; and
           4. suggested improvements in measuring the effectiveness of controls.
        3. On receipt of the results of such reviews, the *Client* will accept any amendments or revisions to the ISMS or Security Management Plan in accordance with the process set out at paragraph [1.4.2.2](#bookmark4).
        4. Any change or amendment which the *Consultant* proposes to make to the ISMS or Security Management Plan (as a result of an *Client’s* request or change to the *services* or otherwise) shall be subject to the early warning procedure and shall not be implemented until accepted in writing by the *Client*.
     5. Testing
        1. The *Consultant* shall conduct Security Tests of the ISMS on an annual basis or as otherwise agreed by the parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the *Client.*
        2. The *Client* shall be entitled to witness the conduct of the Security Tests. The *Consultant* shall provide the *Client* with the results of such tests (in a form accepted by the *Client* in advance) as soon as practicable after completion of each Security Test.
        3. Without prejudice to any other right of audit or access granted to the *Client* pursuant to this contract, the *Client* and/or its authorised representatives shall be entitled, at any time and without giving notice to the *Consultant*, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the *Consultant*'s compliance with the ISMS and the Security Management Plan. The *Client* may notify the *Consultant* of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the carrying out of the *services*. If such tests adversely affect the *Consultant*’s ability to carry out the *services* in accordance with the Scope, the *Consultant* shall be granted relief against any resultant under-performance for the period of the tests.
        4. Where any Security Test carried out pursuant to paragraphs

[1.4.5.2](#bookmark7) or [1.4.5.3](#bookmark8) above reveals any actual or potential Breach of Security, the *Consultant* shall promptly notify the *Client* of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the *Consultant* proposes to make in order to correct such failure or weakness. Subject to the *Client*'s acceptance in accordance with paragraph [(i)](#bookmark3), the *Consultant* shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the *Client* or, otherwise, as soon as reasonably possible. Where the change to the ISMS or Security Management Plan is made to address a non-compliance with the Security Policy or Security Requirements, the change to the ISMS or Security Management Plan is Disallowed Cost.

* 1. Compliance with ISO/IEC 27001
     1. Unless otherwise agreed by the parties, the *Consultant* shall obtain independent certification of the ISMS to ISO/IEC 27001 within 12 months of the date of this contract and shall maintain such certification until the Defects Certificate or a termination certificate has been issued.
     2. In the event that paragraph [1.5.1](#bookmark9) above applies, if certain parts of the ISMS do not conform to Good Industry Practice, or controls as described in ISO/IEC 27002 are not consistent with the Security Policy, and, as a result, the *Consultant* reasonably believes that it is not compliant with ISO/IEC 27001, the *Consultant* shall promptly notify the *Client* of this and the *Client* in its absolute discretion may waive the requirement for certification in respect of the relevant parts.
     3. The *Client* 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.
     4. If, on the basis of evidence provided by such audits, it is the *Client*'s reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the *Consultant*, then the *Client* shall notify the *Consultant* of the same and give the *Consultant* a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to become compliant with the principles and practices of ISO/IEC 27001. If the *Consultant* does not become compliant within the required time then the *Client* has the right to obtain an independent audit against these standards in whole or in part.
     5. If, as a result of any such independent audit as described in paragraph [1.5.4](#bookmark10) the *Consultant* is found to be non-compliant with the principles and practices of ISO/IEC 27001 then the *Consultant* shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the *Client* in obtaining such audit.
  2. Breach of Security
     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. Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 1.6.1, the *Consultant* shall:
        1. immediately take all reasonable steps necessary to:
           1. remedy such breach or protect the integrity of the ISMS against any such potential or attempted breach or threat; and
           2. prevent an equivalent breach in the future.

such steps shall include any action or changes reasonably

required by the *Client*; and

* + - 1. as soon as reasonably practicable provide to the *Client* 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. In this Schedule, the following words shall have the following meanings:

**"Cyber Essentials Scheme"** the Cyber Essentials Scheme developed by the Government which provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats (as may be amended from time to time). Details of the Cyber Essentials Scheme can be found here: <https://www.ncsc.gov.uk/cyberessentials/overview>;

# "Cyber Essentials Basic Certificate"

the certificate awarded on the basis of self-assessment, verified by an independent certification body, under the Cyber Essentials Scheme and is the basic level of assurance;

**"Cyber Essentials Certificate"** Cyber Essentials Basic Certificate, the

Cyber Essentials Plus Certificate or the Cyber Essential Scheme certificate equivalent to be provided by the *Consultant* as set out in the Framework Data Sheet;

**"Cyber Essential Scheme Data"** sensitive and personal information

and other relevant information as referred to in the Cyber Essentials Scheme; and

**"Cyber Essentials Plus Certificate"** the certification awarded on the basis

of external testing by an independent certification body of the *Consultant's* cyber security approach under the Cyber Essentials Scheme and is a more advanced level of assurance.

# CYBER ESSENTIALS OBLIGATIONS

* 1. Where the Scope requires that the *Consultant* provide a Cyber Essentials Certificate prior to the execution of the *services* the *Consultant* shall provide a valid Cyber Essentials Certificate, then on or prior to the commencement of the *services* the *Consultant* delivers to the *Client* evidence of the same. Where the *Consultant* fails to comply with this paragraph it shall be prohibited from commencing the carrying out of the *services* under any contract until such time as the *Consultant* has evidenced to the *Client* its compliance with this paragraph 2.1.
  2. Where the *Consultant* continues to Process Cyber Essentials Scheme Data during the carrying out of the *services* the *Consultant* delivers to the *Client* evidence of renewal of the Cyber Essentials Certificate on each anniversary of the first applicable certificate obtained by the *Consultant* under paragraph 2.1.
  3. Where the *Consultant* is due to Process Cyber Essentials Scheme Data after the commencement of the *services* but before completion of the *services* the *Consultant* delivers to the *Client* evidence of:
     1. a valid and current Cyber Essentials Certificate before the *Consultant* Processes any such Cyber Essentials Scheme Data; and
     2. renewal of the valid Cyber Essentials Certificate on each anniversary of the first Cyber Essentials Scheme certificate obtained by the *Consultant* under paragraph 2.1.
  4. In the event that the *Consultant* fails to comply with paragraphs 2.2 or 2.3 (as applicable), the *Client* reserves the right to terminate this contract for material Default.
  5. The *Consultant* ensures that all sub-contracts with Sub-Consultants who Process Cyber Essentials Data contain provisions no less onerous on the Sub-Consultants than those imposed on the *Consultant* under this contract in respect of the Cyber Essentials Scheme under paragraph 2.1 of this Schedule
  6. This Schedule shall survive termination or expiry of this contract.