STANDARD 'BOILERPLATE' AMENDMENTS

JCT Minor Works with Contractor Design / without Contractor Design

JANUARY 31, 2019

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 eighteen clauses are replicated four times within the NEC, JCT and PPC2000 boilerplate documents. This is one of the **JCT versions** and applies to JCT Minor Works with Contractor Design / without Contractor Design.

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 amended to the contract by way of an additional Schedule of Amendments. This must be referred to in the base contract. 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.

JCT Minor Works with Contractor Design/ without Contractor Design

- Insert a new article into the standard contract document:

  Article 9: Schedule of Amendments

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

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

- Append pages 8 to 43 of this Standard 'Boilerplate' Amendments document to the standard contract document as this Schedule of Amendments.
- 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

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.

2. 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.

3. 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 Contractor must hold subcontractors 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.

4. Official Secrets Act

Contractors 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.

5. 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 Contractor 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.

6. 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 Contractor and further rights for the Client.

7. Security Requirements

This clause is a preface to a schedule requiring the Contractor 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.

8. Tax Compliance

With the inclusion of this clause, the Contractor is under an obligation to notify the Client of relevant Tax Non Compliance. The Contractor must provide more information if the Occasion of Tax Non Compliance occurs prior to defects date (NEC) / Rectification Period (JCT and PPC).

9. Contract (Rights of Third Parties) Act 1999

Excluding third party rights is a common clause in all manner of contracts. The Boilerplate clause removes that exclusion in the case of collateral warranties – a common and often necessary provision in public sector construction. It should be noted that this does not apply to the NEC4 Boilerplate document as the contract directly deals with this under Option X8.

10. Fair Payment

This is a clause also aimed at improving how subcontractors are paid, similarly endorsed in the Government Construction Strategy 2016. Obligations are placed on the Contractor to assess and promptly pay subcontractors, and to ensure that these obligations are also included in their contracts with subcontractors. It should be noted that Fair Payment is a separate clause with the NEC Boilerplate document, whereas within JCT and PPC it is combined with the SME provisions to form 'Conditions of Sub-Contracting' (JCT) or 'Supply Chain' (PPC).

11. 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 Employer's Information Requirements, as well as an option to incorporate a specific type of Protocol, namely the CIC (Construction Industry Council) BIM Protocol. This clause is not replicated in NEC4, which has overlapping mechanisms with the Boilerplate BIM Provision.

12. The Housing Grants, Construction and Regeneration Act 1996 ('Construction Act 2011')

This is an NEC-only clause which expands on an existing provision. If NEC Option Y(UK)2 applies, then the Construction Act also applies to this contract even if the project is in Northern Ireland.

13. Intellectual Property Rights

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

14. MOD DEFCONs

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

15. 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 Contractors to employ a certain amount of SMEs as subcontractors, and to respect a number of other obligations regarding reporting and how they manage these SMEs.

16. 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 Contractors 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 Project Manager to review and discuss a number of measures relating to Apprenticeships.

17. GDPR

With the recent advent of the General Data Protection Regulation, 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.

18. 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 Contractor to provide proof of the required certification at certain stages of the project, and to apply the same obligations to its sub-Contractors.

19. Project Bank Accounts

The Project Bank Accounts scheme is a government policy aimed at enhancing the speed with which payment progresses down the construction supply chain. The scheme has been promoted in the Government Construction Strategies and should be used within central government projects unless there are compelling reasons not to do so. Amended provisions have not been included within this boilerplate document, however their use is encouraged. They should be incorporated using the standard facilities within NEC, JCT and PPC documents.

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

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

Clause 1.1. Definitions

Insert the following new definitions:

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

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

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

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

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

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

DOTAS: is the Disclosure of Tax avoidance Schemes rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the

Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.

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

Employer Data:

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

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

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

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

General Anti-Abuse Rule:

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

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

Intellectual Property Rights or "IPRs":

(a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information;

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

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

(d) all or any goodwill relating or attached thereto.

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

Occasion of Tax Non-Compliance:

- where any tax return of the Contractor submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of:

- A Relevant Tax Authority successfully challenging the Contractor under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;

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

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

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

Prohibited Act:

to directly or indirectly offer, promise or give any person working for or engaged by the Employer or other Contracting Body or any other public body a financial or other advantage to:

- induce that person to perform improperly a relevant function or activity; or

- reward that person for improper performance of a relevant function or activity;

- to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this contract;

- committing any offence:

    - under the Bribery Act 2010 (or any legislation repealed or revoked by such Act)

    - under legislation or common law concerning fraudulent acts; or

    - defrauding, attempting to defraud or conspiring to defraud the Employer; or

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

Request for Information: a request for information or an apparent request under the Code of Practice on Access to government Information, FOIA or the Environmental Information Regulations

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

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

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

1.5 Contracts (Rights of Third Parties) Act 1999

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

Insert new clauses 1.9 to 1.16 as follows:

"**MoD DEFCON Requirements**

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

Freedom of information

1.10.1 The Contractor acknowledges that unless the Architect/Contract Administrator has notified the Contractor that the Employer is exempt from the provisions of the FOIA, the Employer is subject to the requirements of the Code of Practice on Government Information, FOIA and the Environmental Information Regulations. The Contractor shall co-operate with and assist the Employer so as to enable the Employer to comply with its information disclosure obligations.

1.10.2 The Contractor shall:

1.10.2.1 transfer to the Architect/Contract Administrator all Requests for Information that it receives as soon as practicable and in any event within two Working Days of receiving a Request for Information;

1.10.2.2 provide the Architect/Contract Administrator with a copy of all Information in its possession, or power in the form that the Architect/Contract Administrator shall require within five Working Days (or such other period as the Architect/Contract Administrator may specify) of the Architect/Contract Administrator's request;
1.10.2.3 provide all necessary assistance as reasonably requested by the Architect/Contract Administrator to enable the Employer to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations; and
1.10.2.4 procures that its sub-contractors do likewise.
1.10.3 The Employer is responsible for determining in its absolute discretion whether any information is exempt from disclosure in accordance with the provisions of the Code of Practice on Government Information, FOIA or the Environmental Information Regulations.

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

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

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

1.11 **Tax Compliance**

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

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

1.11.2.1 notify the Employer in writing of such fact within 5 days of its occurrence; and
1.11.2.2 promptly provide to the Employer:
1.11.2.2.1 details of the steps which the Contractor is taking to address the Occasions of Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and

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

1.12 **GDPR**

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

1.13 **Confidentiality and Information Sharing**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.13.7.1 to any Crown Body or any other Contracting Bodies. All Crown Bodies or Contracting Bodies receiving such Confidential Information shall be entitled to further disclose the Confidential Information to other Crown Bodies or other Contracting Bodies on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Crown Body or any Contracting Body;

1.13.7.2 to a professional adviser, consultant, contractor, supplier or other person engaged by the Employer or any Crown Body (including any benchmarking organisation) for any purpose connected with this Contract, or any person conducting an Office of Government Commerce gateway review;

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

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

1.13.7.5 for the purpose of the exercise of its rights under this Contract; or

1.13.7.6 to a proposed successor body of the Employer in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under this Contract,

and for the purposes of the foregoing, disclosure of the Contractor's Confidential Information shall be on a confidential basis and subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Employer under this clause 1.13.

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

1.13.9 Nothing in this clause shall prevent either party from using any techniques, ideas or know-how gained during the performance of the contract in the course of its normal business to the extent that this use does not result in a disclosure of the other party's Confidential Information or an infringement of IPR

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

1.13.10.1 to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;
1.13.10.2 to the extent that the Employer (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;

1.14 Prevention of Fraud and Bribery

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

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

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

1.14.2.1 commit a Prohibited Act; and/or

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

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

1.14.3.1 establish, maintain and enforce, and require that its sub-contractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act;

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

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

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

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

1.14.4.2 been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act; and/or

1.14.4.3 received a request or demand for any undue financial or other advantage of any kind in connection with the performance of this Contract or otherwise suspects that any person or Party directly or indirectly connected with this Contract has committed or attempted to commit a Prohibited Act.

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

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

1.15 Security Requirements

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

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

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

1.16 **Cyber Essentials**

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

2.1 Contractor's obligations

Insert new clauses 2.1A to 2.1D as follows:

"2.1A **Admittance to the site**

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

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

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

2.1.A.4 The Contractor shall submit to the Architect/Contract Administrator for acceptance a list of the names of the people for whom passes are required. On acceptance, the Architect/Contract Administrator will issue the passes to the Contractor. Each pass shall be returned to the Architect/Contract Administrator when the employee no longer requires

access to that part of the site or after the Architect/Contract Administrator has given notice that the employee is not to be admitted to the site.

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

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

2.1.B **Legislation and Official secrets**

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

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

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

2.1.C Building Information Modelling

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

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

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

2.1.C.4 In this clause, the Protocol is the CIC Building Information Modelling Protocol, second edition 2018. Terms used in this clause are those defined in the Protocol.

2.1.C.5 Clauses 1, 2, 5, 6, 7, 8, 10 of the Protocol shall form part of this Contract. Clauses 3 and 4 and Appendices 1, 2 and 3 of the Protocol are deemed to be part of the Client's Requirements.

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

2.1.C.6.1 If the Constructor encounters an event which is outside his reasonable control and which prevents him from carrying out the work specified in clauses 4.1.2 to 4.1.4 of the Protocol.

2.1.C.6.2 If the Client revokes a licence granted under clause 6.5 of the Protocol.

2.1.D Copyright and use / Intellectual Property Rights

2.1D In this clause 2.1D 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 Contractor in relation to this Contract.

2.1D.1 The Intellectual Property Rights in all Documents prepared by or on behalf of the Contractor in relation to this Contract and the work executed from them remains the property of the Contractor. The Contractor hereby grants to the Employer an irrevocable, royalty free, non-exclusive licence to use and reproduce the Documents for any and all purposes connected with the construction, use, alterations or demolition of the Site. Such licence entitles the Employer to grant sub-licences to third parties in the same terms as this licence provided always that the Contractor shall not be liable to any 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 Contractor.

2.1D.2 The Employer may assign, novate or otherwise transfer its rights and obligations under the licence granted pursuant to 2.1D.1 to a Crown Body or to anybody (including any private sector body) which performs or carries on any functions and/or activities that previously had been performed and/or carried on by the Employer.

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

2.1D.4 The Contractor waives any moral right to be identified as author of the Documents in accordance with section 77, Copyright Designs and Patents Acts 1988 and any right not to have the Documents subjected to derogatory treatment in accordance with section 8 of that Act as against the Employer or any licensee or assignee of the Employer.

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

2.1D.6 The Contractor warrants to the Employer that he has not granted and shall not (unless authorised by the Employer) grant any rights to any third party to use or otherwise exploit the Documents.

2.1D.7 The Contractor shall supply copies of the Documents to the Architect/Contract Administrator and to the Employer's other contractors and consultants for no additional fee to the extent necessary to enable them to discharge their respective functions in relation to this Contract or related works.

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

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

3.3 Sub-contracting

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

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

3.3.2.5 a provision requiring the sub-contractor to include in each subsubcontract the same requirement (including this requirement to flow down, except that the period for payment is to be not greater than 9 days after the final date for payment in this Contract; and
3.3.2.6 a provision requiring the sub-contractor to assess the amount due to a subsubcontractor without taking into account the amount paid by the Contractor.
3.3.2.7 terms and conditions that are no less favourable than those of this Contract. The Employer shall be entitled to reject sub-contract conditions proposed by the Contractor that are unduly disadvantageous to the sub-contractor"

3.6A **Insert** new clause 3.6A

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

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

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

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

"3.3B Apprenticeships

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

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

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

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

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

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

  (a) work experience placements for 14 to 16 year olds;

  (b) work experience /work trial placements for other ages;

(c) student sandwich/gap year placements;

(d) graduate placements;

(e) vocational training;

(f) basic skills training; and

(g) on site training provision/ facilities."

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

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

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

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

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

DPA 2018 : Data Protection Act 2018

GDPR : the General Data Protection Regulation (Regulation (EU) 2016/679)

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

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

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

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

1. DATA PROTECTION

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

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

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

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

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

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

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

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

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

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

(i) nature of the data to be protected;

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

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

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

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

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

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

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

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

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

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

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

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

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

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

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

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

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

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

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

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

(f) becomes aware of a Data Loss Event.

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

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

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

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

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

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

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

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

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

(b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

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

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

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

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

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

(b) obtain the written consent of the Controller;

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

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

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

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

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

1.15 Where the Parties include two or more Joint Controllers as identified in Schedule [X] in accordance with GDPR Article 26, those Parties shall enter into a Joint Controller Agreement based on the terms outlined in Schedule [Y] in replacement of Clauses 1.1-1.14 for the Personal Data under Joint Control.

Annex A - Part 2: Schedule of Processing, Personal Data and Data Subjects

Schedule [X] Processing, Personal Data and Data Subjects

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

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 Customer is the Controller and the Contractor is the Processor in accordance with Clause 1.1. [Guidance: You may need to vary this section where (in the rare case) the Customer and Contractor have a different relationship. For example where the Parties are Joint Controller of some Personal Data: "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 UNLESS requirement under union or member state law to preserve that type of data	[Describe how long the data will be retained for, how it be returned or destroyed]

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

1. SECURITY PROVISIONS

1.1 Definitions

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

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

"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-contractors in connection with or in relation to the subject matter of this Contract and in respect of which such party is liable to the other;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in this Contract (if any) or as agreed between the parties;
"Employer Premises"	means premises owned, controlled or occupied by the Employer or its Affiliates which are made available for use by the Contractor or its sub-contractors for carrying out of the Works (or any of them) on the terms set out in this Contract or any separate agreement or licence;
"Employer System"	the Employer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Employer or the Contractor in connection with this Contract which is owned by or licensed to the Employer by a third party and which interfaces with the Contractor System or which is necessary for the Employer to benefit from the Works;
"Environmental Information Regulations"	the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issues by the Information Commissioner or relevant Government Department in relation to such regulations;
"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such legislation;
"Good Industry Practice"	the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector;

"ICT"	information and communications technology;
"ICT Environment"	the Employer System and the Contractor System;
"Impact Assessment"	an assessment of a Change Request;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Information Assets Register"	the register of information assets to be created and maintained by the Contractor throughout the carrying out of the Works as described in the Contract (if any) or as otherwise agreed between the parties;
"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 Works;
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the Works but excluding know how already in the Contractor's or the Employer's possession before this contract;
"List x"	means, in relation to a sub-contractor, one who has been placed on List x in accordance with Ministry of Defence guidelines and procedures, due to that Sub contractor undertaking work on its premises marked as CONFIDENTIAL or above;
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"Process"	has the meaning given to it under the Data Protection Legislation but, for the purposes of this contract, it shall include both manual and automatic processing;
"Protectively Marked"	shall have the meaning as set out in the Security Policy Framework.
"Regulatory Bodies"	those government departments and regulatory, statutory

	and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Contract or any other affairs of the Employer and "Regulatory Body" shall be construed accordingly;
"Request for Information"	a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations;
"Security Management Plan"	the Contractor's security plan prepared pursuant to paragraph 1.5.3 of this Schedule (Security Management Plan) an outline of which is set out in Appendix 1 of this schedule (Security Management Plan);
"Security Policy Framework"	means the Cabinet Office Security Policy Framework (available from the Cabinet Office Security Policy Division);
"Security Requirements"	means the requirements in the Contract relating to security of the carrying out of the Works (if any) or such other requirements as the Employer may notify to the Contractor 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]
"Sites"	any premises at which the Works are carried out or from which the Contractor manages, organises or otherwise directs the provision or the use of the Works or where any part of the Contractor System is situated or where any physical interface with the Employer System takes place;
"Software"	Specially Written Software, Contractor Software and Third Party Software;
"Specially Written Software"	any software created by the Contractor (or by a third party on behalf of the Contractor) specifically for the purposes of this contract;
"Staff Vetting Procedures"	the Employer's procedures and departmental policies for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures, including, but not limited to, the provisions of the Official Secrets Act 1911 to 1989;

"Statement of Applicability"	shall have the meaning set out in ISO/IEC 27001 and as agreed by the parties during the procurement phase;
"Standards"	the British or international standards,[Employer's internal policies and procedures, Government codes of practice and guidance together with any other specified policies or procedures referred to in this Contract (if any) or as otherwise agreed by the parties;
"Third Party Software"	software which is proprietary to any third party other than an Affiliate of the Contractor which is or will be used by the Contractor for the purposes of carrying out of the Works; and

1.2 Introduction

1.2.1 This schedule covers:

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

1.2.1.2 wider aspects of security relating to carrying out of the Works;

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

1.2.1.4 the creation and maintenance of the Security Management Plan;

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

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

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

1.3 Principles of Security

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

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

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

1.3.2.2 complies with the Security Policy;

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

1.3.2.4 meets any specific security threats to the ISMS; and

1.3.2.5 complies with ISO/IEC27001 and ISO/IEC27002 in accordance with paragraph **Error! Reference source not found.** of this schedule;

1.3.2.6 complies with the Security Requirements; and

1.3.2.7 complies with the Employer's ICT standards.

1.3.3 The references to standards, guidance and policies set out in paragraph **Error! Reference source not found.** shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, from time to time.

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

1.4 ISMS and Security Management Plan

1.4.1 Introduction:

1.4.1.1 The Contractor shall develop, implement, operate, maintain and continuously improve and maintain an ISMS which will, without prejudice to paragraph **Error! Reference source not found.**, be approved, by the Architect/Contract Administrator, tested in accordance with the provisions relating to testing as set out in the Contract (if any) or as otherwise agreed between the parties, periodically updated and audited in accordance with ISO/IEC 27001.

1.4.1.2 The Contractor shall develop and maintain a Security Management Plan in accordance with this Schedule to apply during the carrying out of the Works.

1.4.1.3 The Contractor shall comply with its obligations set out in the Security Management Plan.

1.4.1.4 Both the ISMS and the Security Management Plan shall, unless otherwise specified by the Employer, aim to protect all aspects of the Works and all processes associated with carrying out the Works, including the Site, the Contractor System and any ICT, information and data (including the Employer Confidential Information and the Employer Data) to the extent used by the Employer or the Contractor in connection with this contract.

1.4.2 Development of the Security Management Plan:

1.4.2.1 Within 20 Working Days after the Contract Date and in accordance with paragraph **Error! Reference source not found.** (Amendment and Revision), the Contractor will prepare and deliver to the Architect/Contract Administrator for approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan set out in Appendix 2 of this Part 2 of this Schedule.

1.4.2.2 If the Security Management Plan, or any subsequent revision to it in accordance with paragraph **Error! Reference source not found.** (Amendment and Revision), is approved by the Architect/Contract Administrator it will be adopted immediately and will replace the previous version of the Security Management Plan at Appendix 2 of this Part 2 of this Contract Schedule. If the Security Management Plan is not approved by the Architect/Contract Administrator the Contractor shall amend it within 10 Working Days or such other period as the parties may agree in writing of a notice of non-approval from the Architect/Contract Administrator and re-submit to the Architect/Contract Administrator for approval. The parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the parties may agree in writing) from the date of its first submission to the Architect/Contract Administrator. If the Architect/Contract Administrator does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Architect/Contract Administrator pursuant to this paragraph **Error! Reference source not found.** of this

schedule may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in paragraph **Error! Reference source not found.** shall be deemed to be reasonable.

1.4.3 Content of the Security Management Plan:

1.4.3.1 The Security Management Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Works and all processes associated with carrying out the Works and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Works comply with the provisions of this schedule (including the principles set out in paragraph **Error! Reference source not found.**);

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

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

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

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

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

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Contractor System, the Works and/or associated processes;

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

(d) any reasonable request by the Architect/Contract Administrator.

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

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

(b) updates to the risk assessments;

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

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

1.4.4.3 On receipt of the results of such reviews, the Architect/Contract Administrator will approve any amendments or revisions to the ISMS or Security Management Plan in accordance with the process set out at paragraph **Error! Reference source not found.**.

1.4.4.4 Any change or amendment which the Contractor proposes to make to the ISMS or Security Management Plan (as a result of a Architect/Contract Administrator's request or change to the Works or otherwise) shall be subject to the early warning procedure and shall not be implemented until approved in writing by the Architect/Contract Administrator.

1.4.5 Testing

1.4.5.1 The Contractor shall conduct tests of the ISMS ("Security Tests") on an annual basis or as otherwise agreed by the parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Architect/Contract Administrator.

1.4.5.2 The Architect/Contract Administrator shall be entitled to witness the conduct of the Security Tests. The Contractor shall provide the Architect/Contract Administrator with the results of such

tests (in a form approved by the Employer in advance) as soon as practicable after completion of each Security Test.

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

1.4.5.4 Where any Security Test carried out pursuant to paragraphs **Error! Reference source not found.** or **Error! Reference source not found.** above reveals any actual or potential Breach of Security, the Contractor shall promptly notify the Architect/Contract Administrator of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to the Architect/Contract Administrator's approval in accordance with paragraph **Error! Reference source not found.**, the Contractor shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the Architect/Contract Administrator or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan to address a non-compliance with the Security Policy or Security Requirements the change to the ISMS or Security Management Plan shall be at no cost to the Employer.

1.5 Compliance with ISO/IEC 27001

1.5.1 Unless otherwise agreed by the parties, the Contractor shall obtain independent certification of the ISMS to ISO/IEC 27001 within 12 months of the Contract Date and shall maintain such certification for the duration of the contract.

1.5.2 In the event that paragraph **Error! Reference source not found.** above applies, if certain parts of the ISMS do not conform to Good Industry

Practice, or controls as described in ISO/IEC 27002 are not consistent with the Security Policy, and, as a result, the Contractor reasonably believes that it is not compliant with ISO/IEC 27001, the Contractor shall promptly notify the Architect/Contract Administrator of this and the Employer in its absolute discretion may waive the requirement for certification in respect of the relevant parts.

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

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

1.5.5 If, as a result of any such independent audit as described in paragraph **Error! Reference source not found.** the Contractor is found to be non-compliant with the principles and practices of ISO/IEC 27001 then the Contractor shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Employer in obtaining such audit.

1.6 Breach of Security

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

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

1.6.2.1 immediately take all reasonable steps necessary to:

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

(b) prevent an equivalent breach in the future.

such steps shall include any action or changes reasonably required by the Architect/Contract Administrator; and

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

Appendix 1 – Security Policy

[Guidance Note: Append Security Policy]

Appendix 2 – Security Management Plan

[Guidance Note: Append Security Management Plan]

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

CYBER ESSENTIALS SCHEME

1. DEFINITIONS

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

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

2. CYBER ESSENTIALS OBLIGATIONS

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

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

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

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

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

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

2.5 The Contractor shall ensure that all sub-contracts with sub-contractors who Process Cyber Essentials Data contain provisions no less onerous on the sub-contractors than those imposed on the Contractor under this Contract in respect of the Cyber Essentials Scheme under paragraph 2.1 of this Schedule

2.6 This Schedule shall survive termination or expiry of this Contract