STANDARD ‘BOILERPLATE’ AMENDMENTS

Materials Supply/Supply and Install Conditions – Longer Form

[ ] 2021

CABINET OFFICE

Crown Commercial Service

The standardised ‘boilerplate’ amendments project addresses a need to simplify the inclusion of government-specific clauses. 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.

This is the **Materials Supply/Supply and Install Conditions – Longer Form 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 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.

**Materials Supply/Supply and Install Conditions – Longer Form**

* In the Particulars section “Special Conditions” insert:

The Special Conditions are as detailed in the appended Schedule of Amendments.

* Append pages 8 to 27 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 and amend terms as provided by guidance notes.
* Add additional, project specific amendments in the normal way.

Table of Contents

# Summary of Clauses 5

Definitions 7

28A Security Requirements 8

28B Intellectual Property Rights 9

28C HMRC Requirements…………………………………………………………………………9

28D MOD DEFCONS 9

28E Small and Medium Enterprises (SMEs) 9

28F Apprenticeships 10

28G Change of Control…………………………………………………………………………..11

28H Financial Standing……………………………………………………………………….….11

28I Financial Distress………………………………………………………………………….....11

28J Cyber Essentials 11

# Schedules

Financial Distress……………………………………………………………………..……….....12

Security Provisions 16

Cyber Essentials 26

# 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. Security Requirements

This clause is a preface to a schedule requiring the Supplier to create and maintain a comprehensive Information Security Management System. This must be agreed with the Purchaser, 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. Intellectual Property Rights

This indicates that the Supplier provides to the Purchaser an irrevocable, royalty free and non- exclusive licence to use the Intellectual Property of the Supplier. The Purchaser may transfer these rights in a variety of circumstances, and the Supplier is subject to a number of additional obligations. It would be used where the Supplier is providing bespoke design for the products.

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 Suppliers 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.

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 Purchasers to ensure that Suppliers 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 Purchaser 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 Purchaser 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 Supplier’s financial standing which affects or may affect the Supplier’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 Supplier’s credit rating, requiring the Supplier to provide a satisfactory continuity plan for approval. It also allows for termination if the Supplier fails to notify a significant downgrade in its credit rating, or fails to produce or comply with an approved continuity plan.

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 Supplier to provide proof of the required certification at certain stages of the project, and to apply the same obligations to its subcontractors.

1. 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.

**SCHEDULE OF AMENDMENTS TO NEC4 SUPPLY CONTRACT**

# Definitions and interpretation

Insert additional defined terms.

‘**Change of Control**’ is a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;

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

‘**Intellectual Property Rights**’ or ‘I**PRs**’ means

* + - 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.

Personal Data has the meaning given to it in the Data Protection Legislation.

Purchaser 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 Supplier by or on behalf of the Purchaser,

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

• which are any Personal Data for which the Purchaser is the Data Controller to the extent that such Personal Data is held or processed by the Supplier.

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

# Security Requirements

28A The Supplier complies with, and shall procure the compliance of the Supplier’s employees, sub-contractors and suppliers, with the Security Policy and the Security Management Plan produced by the Supplier and the Supplier shall ensure that the Security Management Plan fully complies with the Security Policy and Contract Schedule [Guidance: insert schedule ref here].

# Intellectual Property Rights

# 28B.1 In this clause 28B ‘Documents’ 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 Supplier in relation to this Contract.

28B.2 The Intellectual Property Rights in all Documents prepared by or on behalf of the Supplier in relation to this Contract and the work executed from them remain the property of the Supplier. The Supplier hereby grants to the Purchaser an irrevocable, royalty free, non-exclusive licence to use and reproduce the Documents for any and all purposes connected with the installation, use, maintenance, alteration or modification of the Products and the construction, alteration, maintenance and demolition of the Project. Such licence entitles the Purchaser to grant sub-licences to third parties in the same terms as this licence provided always that the Supplier 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 Supplier.

28B.3 The Purchaser may assign novate or otherwise transfer its rights and obligations under the licence granted pursuant to clause 28B.2 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 Purchaser.

28B.4 In the event that the Supplier does not own the copyright or any Intellectual Property Rights in any Document the Supplier shall use all reasonable endeavours to procure the right to grant such rights to the Purchaser 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 Supplier is unable to procure the right to grant to the Purchaser in accordance with the foregoing the Supplier shall procure that the third party grants a direct licence to the Purchaser on industry acceptable terms.

28B.5 The Supplier 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 Purchaser or any licensee or assignee of the Purchaser.

28B.6 In the event that any act unauthorised by the Purchaser infringes a moral right of the Supplier in relation to the Documents the Supplier undertakes, if the Purchaser so requests and at the Purchaser's expense, to institute proceedings for infringement of the moral rights.

28B.7 The Supplier warrants to the Purchaser that it has not granted and shall not (unless authorised by the Purchaser) grant any rights to any third party to use or otherwise exploit the Documents.

28B.8 The Supplier shall supply copies of the Documents to the Purchaser and to the Purchaser’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 goods or services.

28B.9 After the termination or conclusion of the Supplier’s employment hereunder, the Supplier shall supply the Purchaser with copies and/or computer discs of such of the Documents as the Purchaser may from time to time request and the Purchaser shall pay the Supplier’s reasonable costs for producing such copies or discs.

28B.10 In Performance the Supplier shall not infringe any Intellectual Property Rights of any third party. The Supplier shall indemnify the Purchaser against claims, proceedings, compensation and costs arising from an infringement or alleged infringement of the Intellectual Property Rights of any third party.

# HMRC Requirements

28C

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

# MoD DEFCON Requirements

28D

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)

# Small and Medium Sized Enterprises (SMEs)

28E.1The Supplier is required to take all reasonable steps to engage SMEs as sub-contractors and to seek to ensure that no less than [ ]% of sub-contractors are SMEs or that a similar proportion of the Defined Cost is undertaken by SMEs.

28E.2 The Supplier is required to report to the Purchaser in its regular contract management monthly reporting cycle the numbers of SMEs engaged as sub-contractors and the value of the Defined Cost that has been undertaken by SMEs.

28E.3 Where available, the Supplier is required to tender its sub-contracts using the same online electronic portal as was provided by the Purchaser for the purposes of tendering this Contract.

28E.4 The Supplier is to ensure that the terms and conditions used to engage sub-contractors are no less favourable than those of this contract. The Supplier shall provide copies of the proposed terms of engagement for its sub-contractors for approval by the Purchaser and the Purchaser may withhold its approval if the sub-contract documents proposed by the Supplier are unduly disadvantageous to the sub-contractor.

# Apprenticeships

28F.1 The Supplier shall take all reasonable steps to employ apprentices, and reports to the Purchaser the numbers of apprentices employed and the wider skills training provided, during Performance.

28F.2 The Supplier shall take 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 Performance (which may include support staff and sub-contractors) are provided by people on formal apprenticeship programmes.

28F.3 The Supplier shall make available to its people and sub-contractors working on the contract, information about the Government’s Apprenticeship programme and wider skills opportunities.

28F.4 The Supplier shall provide any further skills training opportunities that are appropriate for its people engaged in Performance.

28F.5 The *Supplier shall* provide a report detailing the following measures in its regular contract management monthly reporting cycle and is prepared to discuss apprenticeships at its regular meetings with the Purchas*er*

28F.5.1 the number of people during the reporting period employed on the Contract, including support staff and sub-contractors,

28F.5.2 the number of apprentices and number of new starts on apprenticeships directly initiated through this contract,

28F.5.3 the percentage of all people taking part in an apprenticeship programme,

28F.5.4 if applicable, an explanation from the Supplier as to why it is not managing to meet the specified percentage target,

28F.5.5 actions being taken to improve the take up of apprenticeships and

28F.5.6 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.

# Change of Control

28G.1 The Supplier shall notify the Purchaser immediately in writing and as soon as the Supplier 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 Supplier shall ensure that any notification sets out full details of the Change of Control including the circumstances suggesting and/or explaining the Change of Control.

28G.2 The Purchaser may terminate the Supplier’s engagement under the Contract (which shall take effect as termination for the Supplier being Insolvent) within six months from

28G.2.1 being notified in writing that a Change of Control is anticipated or is in contemplation or has occurred; or

28G.2.2 where no notification has been made, the date that the Purchaser 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.

# Financial Standing

28H.1 The Purchaser may terminate the Supplier’s engagement under the Contract (which shall take effect as termination for the Supplier being Insolvent) where in the reasonable opinion of the Purchaser there is a material detrimental change in the financial standing and/or the credit rating of the Supplier which:

28H.1.1 adversely impacts on the Supplier’s ability to perform its obligations under this Contract; or

28H.1.2 could reasonably be expected to have an adverse impact on the Supplier’s ability to perform its obligations under this Contract.

# Financial Distress

28I The Supplier shall comply with the provisions of Schedule [Guidance: insert schedule ref here] (Financial Distress) in relation to the assessment of the financial standing of the Supplier and the consequences of a change to that financial standing.

# Cyber Essentials

28J The Purchaser and the Supplier 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 Supplier 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 Supply Continuity Plan" means a plan setting out how the Supplier 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 Supplier warrants and represents to the Purchaser for the benefit of the Purchaser that as at the Contract Date the long-term credit ratings issued for the Supplier by the Rating Agency.

2.2. The Supplier shall promptly notify (or procures that its auditors promptly notify) the Purchaser if there is any significant downgrade in the credit rating issued by any Rating Agency for the Supplier (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 Supplier, the Supplier shall ensure that the Supplier’s auditors thereafter provide the Purchaser within 14 days of a written request by the Purchaser with written calculations of the quick ratio for the Supplier at such date as may be requested by the Purchaser. 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 Supplier

B. is the value of all marketable securities held by the Supplier 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 Supplier and

D. is the value at the relevant date of the current liabilities of the Supplier.

2.4. The Supplier shall:

* regularly monitor the credit ratings of the Supplier with the Rating Agencies and
* promptly notify (or shall procure that its auditors promptly notify) the Purchaser 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 Supplier 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 Supplier shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated the Supplier 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 Supplier dropping below the applicable Credit Rating Threshold;

3.1.2. the Supplier 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 Supplier;

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

3.1.5. a sub-contractor or supplier notifying the Purchaser that the Supplier 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 Supplier with respect to financial indebtedness or obligations under this Contract;
* non-payment by the Supplier of any financial indebtedness; any financial indebtedness of the Supplier becoming due as a result of an event of default
* the cancellation or suspension of any financial indebtedness in respect of the Supplier in each case which the Purchaser reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of the Supplier in accordance with this Contract

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

3.2. The Supplier shall:

3.2.1 at the request of the Purchaser meet the Purchaser as soon as reasonably practicable (and in any event within three Business Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Purchaser may permit and notify to the Supplier 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 Purchaser reasonably believes (taking into account any discussions and representations under paragraph 3.2.1) that the Financial Distress Event could impact on the Supplier’s continued performance in accordance with this Contract:

* submit to the Purchaser for approval, a draft Financial Distress Supply 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 Purchaser may permit and notify to the Supplier in writing)
* provide such financial information relating to the Supplier as the Purchaser may reasonably require.

3.3. The Purchaser shall not withhold approval of a draft Financial Distress Supply Continuity Plan unreasonably. If the Purchaser does not approve the draft Financial Distress Supply Continuity Plan, the Purchaser shall inform the Supplier of the reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Supply Continuity Plan, which the Supplier shall resubmit to the Purchaser 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 Supply Continuity Plan is approved by the Purchaser or referred to the dispute resolution procedure.

3.4. If the *Purchaser* considers that the draft Financial Distress Supply 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 Purchaser may either agree a further time period for the development and agreement of the Financial Distress Supply Continuity Plan or escalate any issues with the draft Financial Distress Supply Continuity Plan using the dispute resolution procedure.

3.5. Following approval of the Financial Distress Supply Continuity Plan by the Purchaser the Supplier shall:

* review on a regular basis (which shall not be less than monthly) the Financial Distress Supply 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 Supply Continuity Plan is not adequate or up to date in, submit an updated Financial Distress Supply Continuity Plan to the Purchaser for approval, and the provisions of shall apply to the review and approval process for the updated Financial Distress Supply Continuity Plan; and
* comply with the Financial Distress Supply Continuity Plan (including any updated Financial Distress Supply Continuity Plan).

3.6. Where the Supplier 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 Supplier notifies the Purchaser and subject to the agreement of the Purchaser, the Supplier shall be relieved of its obligations under paragraph 3.

**4. Termination rights**

4.1. The Purchaser may terminate Supplier’s engagement under the Contract (which shall take effect as termination for the Supplier being Insolvent) if

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

**5. Primacy of credit ratings**

5.1. Without prejudice to the Supplier’s obligations and the Purchaser’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 Supplier is relieved automatically of its obligations under paragraph 3 and
* the Purchaser is not entitled to require the Supplier to provide financial information in accordance with paragraph 2.3.

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

Supplier Credit current rating (long term) [ ]

Credit Rating Threshold [ ]

# 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 goods or services the Purchaser Premises, the Sites, the Supplier System and/or any ICT, information or data (including the Confidential Information and the Purchaser Data) used by the Purchaser and/or the Supplier 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 Purchaser Data), including any copies of such information or data, used by the Purchaser and/or the Supplier in connection with this Contract. |
| **"Clearance"** | means national security clearance and employment checks undertaken by and/or obtained from the Defence Vetting Agency; |
| **"Supplier Equipment"** | the hardware, computer and telecoms devices and equipment supplied by the Supplier or its sub-contractors (but not hired, leased or loaned from the Purchaser) for the purposes of Performance; |
| **"Supplier Software"** | software which is proprietary to the Supplier, including software which is or will be used by the Supplier for the purposes of Performance; |
| **"Supplier System"** | the information and communications technology system used by the Supplier in Performance including the Software, the Supplier Equipment and related cabling (but excluding the Purchaser 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; |
| **"Purchaser Premises"** | means premises owned, controlled or occupied by the Purchaser or its Affiliates which are made available for use by the Supplier or its sub-contractors for Performance on the terms set out in this Contract or any separate agreement or licence; |
| **"Purchaser System"** | the Purchaser's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Purchaser or the Supplier in connection with this contract which is owned by or licensed to the Purchaser by a third party and which interfaces with the Supplier System or which is necessary for the Purchaser to receive the Products; |
| **"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 Purchaser System and the Supplier 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 Supplier throughout Performance 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 goods or services; |
| **"Know-How"** | all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the goods or services but excluding know how already in the Supplier’s or the Purchaser’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 *Purchaser* 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 Supplier'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); |
| **"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 Performance (if any) or such other requirements as the Purchaser may notify to the Supplier 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, Supplier Software and Third Party Software; |
| **"Specially Written Software"** | any software created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this contract; |
| **"Staff Vetting Procedures"** | the Purchaser'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, Purchaser'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 *Supplier* which is or will be used by the *Supplier* for the purposes of Performance*.* |

* 1. Introduction
     1. This schedule covers:
        1. principles of protective security to be applied in Performance;
        2. wider aspects of security relating to Performance;
        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 Supplier acknowledges that the Purchaser places great emphasis on the confidentiality, integrity and availability of information and consequently on the security provided by the ISMS.
     2. The Supplier 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 Purchaser’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 Supplier shall give an early warning to the Purchaser of such inconsistency immediately upon becoming aware of the same, and the Purchaser shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.
  1. ISMS and Security Management Plan
     1. Introduction:
        1. The Supplier 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 Supply manager, tested in accordance with the provisions relating to testing as set out in the contract (if any) or as otherwise agreed between the Parties, periodically updated and audited in accordance with ISO/IEC 27001.
        2. The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule to apply during Providing the Goods and Services.
        3. The Supplier 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 Purchaser, aim to protect all aspects of the Products and all processes associated with Performance including the construction, use, alterations or destruction of the Products, the Supplier System and any ICT, information and data (including the Purchaser Confidential Information and the Purchaser Data) to the extent used by the Purchaser or the Supplier in connection with this Contract.
     2. Development of the Security Management Plan:
        1. Within 20 Business Days after the date of the Contract and in accordance with paragraph [1.4.4](#bookmark6) (Amendment and Revision), the Supplier will prepare and deliver to the Purchaser 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 Purchaser 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 Purchaser the Supplier shall amend it within 10 Business Days or such other period as the parties may agree in writing of a notice of non- acceptance from the Purchaser and re-submit to the Purchaser for accepted. 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 Business Days (or such other period as the parties may agree in writing) from the date of its first submission to the Purchaser. If the Purchaser 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 Purhcaser 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 Supplier in relation to all aspects of the Products and all processes associated with Performance and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Productscomply 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 the Contract to those incorporated in the Supplier’s ISMS at the date notified by the Purchaser to the Supplier for the Supplier 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 Supplier and the Purchaser engaged in Performance and shall only reference documents which are in the possession of the Purchaser 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 Supplier annually or from time to time to reflect:
           1. emerging changes in Good Industry Practice;
           2. any change or proposed change to the Supplier System, the Products and/or associated processes;
           3. any new perceived or changed security threats; and
           4. any reasonable request by the Purchaser.
        2. The Supplier will provide the Purchaser 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 Purchaser. 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 Purchaserwill 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. The Supplier shall provide early warning of any change or amendment which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a Purchaser’s request or change to the Productsor otherwise) and this shall not be implemented until accepted in writing by the Purchaser.
     5. Testing
        1. The Supplier 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 Purchaser.
        2. The Purchaser shall be entitled to witness the conduct of the Security Tests. The Supplier shall provide the Purchaser with the results of such tests (in a form accepted by the Purchaser 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 *Purchaser* pursuant to this contract, the Purchaser and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Purchaser may notify the Supplier 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 Performance. If such tests adversely affect the Supplier’s ability to carry out Performance, the Supplier 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 Supplier shall promptly notify the Purchaser of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Purchaser's acceptance in accordance with paragraph [(i)](#bookmark3), the Supplier shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the Purchaser 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 Supplier shall not be entitled to any payment in respect of the cost of such change to the ISMS or Security Management Plan.

* 1. Compliance with ISO/IEC 27001
     1. Unless otherwise agreed by the parties, the Supplier shall obtain independent certification of the ISMS to ISO/IEC 27001 within 12 months of the date of the Contract and shall maintain such certification until the expiry of 12 months from the date of completion of delivery and unloading and (if applicable) or the date of termination of the Supplier’s engagement under the Contract (whichever is the later).
     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 Supplier reasonably believes that it is not compliant with ISO/IEC 27001, the Supplier shall promptly notify the Purchaser of this and the Purchaser in its absolute discretion may waive the requirement for certification in respect of the relevant parts.

* + 1. The Purchaser shall be entitled to carry out such regular security audits as may be required and in accordance with Good Industry Practice, in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001.
    2. If, on the basis of evidence provided by such audits, it is the Purchaser’s reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the Supplier, then the Purchaser shall notify the Supplier of the same and give the Supplier 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 Supplier does not become compliant within the required time then the Purchaser has the right to obtain an independent audit against these standards in whole or in part.
    3. If, as a result of any such independent audit as described in paragraph [1.5.4](#bookmark10) the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 then the Supplier 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 Purchaser in obtaining such audit.
  1. 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 Supplier 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 Purchaser; and

* + - 1. as soon as reasonably practicable provide to the Purchaserfull 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 al 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 Supplieras 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 Supplier's cyber security approach under the Cyber Essentials Scheme and is a more advanced level of assurance. |

# CYBER ESSENTIALS OBLIGATIONS

* 1. Where Performance requires that the Supplier provide a Cyber Essentials Certificate prior to the execution of the service the Supplier shall provide a valid Cyber Essentials Certificate, then on or prior to the commencement of the service the Supplier delivers to the Purchaser evidence of the same. Where the Supplier fails to comply with this paragraph it shall be prohibited from commencing Performance under any contract until such time as the Supplier has evidenced to the Purchaser its compliance with this paragraph 2.1.
  2. Where the Supplier continues to Process Cyber Essentials Scheme Data during Performance the Supplier shall deliver to the Purchaser evidence of renewal of the Cyber Essentials Certificate on each anniversary of the first applicable certificate obtained by the Supplier under paragraph 2.1.
  3. Where the Supplier is due to Process Cyber Essentials Scheme Data after the commencement of Performance but before completion of Performance the Supplier delivers to the Purchaser evidence of:
     1. a valid and current Cyber Essentials Certificate before the *Supplier* 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 Supplier under paragraph 2.1.
  4. In the event that the Supplier fails to comply with paragraphs 2.2 or 2.3 (as applicable), the Purchaser reserves the right to terminate the Supplier’s engagement under this Contract for material default.
  5. The Supplier 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 Supplier 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.