



**DEFENCE MUNITIONS**

**DM/00181**

**DM BEITH APPRENTICE TRAINING SERVICES 2024**

THIS DOCUMENT IS THE PROPERTY OF  
HER BRITANNIC MAJESTY'S GOVERNMENT,  
And is issued for the information of such persons only as need.  
to know its contents in the course of their duties.  
Any person finding this document should hand it to a British  
Forces unit or to a police station for its safe return to the  
MINISTRY OF DEFENCE, D MOD SY, LONDON SW1 2HB,  
With particulars of how and where found.

THE UNAUTHORISED RETENTION OR DESTRUCTION OF THE DOCUMENT IS AN OFFENCE  
UNDER THE OFFICIAL SECRETS ACTS OF 1911–1989

## Standardised Contracting Terms

**SC1A** (Edn 06/24)

### 1 Definitions - In the Contract:

**Article** means, in relation to Clause 9 only, an object which during production is given a special shape, surface or design which determines its function to a greater degree than does its chemical composition;

**The Authority** means the Secretary of State for Defence of the United Kingdom of Great Britain and Northern Ireland, (referred to in this document as "the Authority"), acting as part of the Crown;

**Business Day** means 09:00 to 17:00 Monday to Friday, excluding public and statutory holidays;

**Contract** means the agreement concluded between the Authority and the Contractor, including all terms and conditions, associated purchase order, specifications, plans, drawings, schedules and other documentation, expressly made part of the agreement in accordance with Clause 2.c;

**Contractor** means the person, firm or company specified as such in the purchase order. Where the Contractor is an individual or a partnership, the expression shall include the personal representatives of the individual or of the partners, as the case may be;

**Contractor Deliverables** means the goods and / or services including packaging (and supplied in accordance with any QA requirements if specified) which the Contractor is required to provide under the Contract in accordance with the schedule to the purchase order;

**Effective Date of Contract** means the date stated on the purchase order or, if there is no such date stated, the date upon which both Parties have signed the purchase order;

**Firm Price** means a price excluding Value Added Tax (VAT) which is not subject to variation;

**Government Furnished Assets (GFA)** is a generic term for any MOD asset such as equipment, information or resources issued or made available to the Contractor in

connection with the Contract by or on behalf of the Authority;

**Hazardous Contractor Deliverable** means a Contractor Deliverable or a component of a Contractor Deliverable that is itself a hazardous material or substance or that may in the course of its use, maintenance, disposal, or in the event of an accident, release one or more hazardous materials or substances and each material or substance that may be so released;

**Issued Property** means any item of Government Furnished Assets (GFA), including any materiel issued or otherwise furnished to the Contractor in connection with the Contract by or on behalf of the Authority;

**Legislation** means in relation to the United Kingdom any Act of Parliament, any subordinate legislation within the meaning of section 21 of the Interpretation Act 1978, any exercise of Royal Prerogative or any enforceable community right within the meaning of Section 2 of the European Communities Act 1972.

**Mixture** means a mixture or solution composed of two or more substances;

**Notices** means all notices, orders, or other forms of communication required to be given in writing under or in connection with the Contract;

**Parties** means the Contractor and the Authority, and Party shall be construed accordingly;

**PPT** means a tax called "plastic packaging tax" charged in accordance with Part 2 of the Finance Act 2021;

**PPT Legislation** means the legislative provisions set out in Part 2 and Schedules 9-15 of the Finance Act 2021 together with any secondary legislation made under powers contained in Part 2 of the Finance Act 2021. This includes, but is not limited to, The Plastic Packaging Tax (Descriptions of Products) Regulations 2021 and The Plastic Packaging Tax (General) Regulations 2022;

**Plastic Packaging Component(s)** shall have the same meaning as set out in Part 2 of the Finance Act 2021 together with any associated secondary legislation;

**Sensitive Information** means the

information listed as such in the purchase order, being information notified by the Contractor to the Authority, which is acknowledged by the Authority as being sensitive, at the point at which the Contract is entered into or amended (as relevant) and remains sensitive information at the time of publication;

**Substance** means a chemical element and its compounds in the natural state or obtained by any manufacturing process, including any additive necessary to preserve its stability and any impurity deriving from the process used, but excluding any solvent which may be separated without affecting the stability of the substance or changing its composition;

**Transparency Information** means the content of this Contract in its entirety, including from time to time agreed changes to the Contract, except for (i) any information which is exempt from disclosure in accordance with the Freedom of Information Act 2000 (FOIA) or the Environmental Information Regulations Act 2004 (EIR), which shall be determined by the Authority, and (ii) any Sensitive Information.

## 2 General

- a. The Contractor shall comply with all applicable Legislation, whether specifically referenced in this Contract or not.
- b. Any variation to the Contract shall have no effect unless expressly agreed in writing and signed by both Parties.
- c. If there is any inconsistency between these terms and conditions and the purchase order or the documents expressly referred to therein, the conflict shall be resolved according to the following descending order of priority:
  - (1) the terms and conditions;
  - (2) the purchase order; and
  - (3) the documents expressly referred to in the purchase order.
- d. Neither Party shall be entitled to assign the Contract (or any part thereof) without the prior written consent of the other Party.
- e. Failure or delay by either Party in enforcing or partially enforcing any provision of the Contract shall not be

construed as a waiver of its rights or remedies. No waiver in respect of any right or remedy shall operate as a waiver in respect of any other right or remedy.

f. The Parties to the Contract do not intend that any term of the Contract shall be enforceable by virtue of the Contracts (Rights of Third Parties) Act 1999 by any person that is not a Party to it.

g. The Contract and any non-contractual obligations arising out of or in connection with it shall be governed by and construed in accordance with English Law, and subject to Clause 16 and without prejudice to the dispute resolution procedure set out therein, the Parties submit to the exclusive jurisdiction of the English courts. Other jurisdictions may apply solely for the purpose of giving effect to this Clause 2.g and for enforcement of any judgement, order or award given under English jurisdiction.

## 3 Application of Conditions

- a. The purchase order, these terms and conditions and the specification govern the Contract to the entire exclusion of all other terms and conditions. No other terms or conditions are implied.
- b. The Contract constitutes the entire agreement and understanding and supersedes any previous agreement between the Parties relating to the subject matter of the Contract.

## 4 Disclosure of Information

Disclosure of information under the Contract shall be managed in accordance with DEFCON 531 (SC1).

## 5 Transparency

- a. Notwithstanding any other condition of this Contract, and in particular Clause 4, the Contractor understands that the Authority may publish the Transparency Information to the general public.
- b. Subject to Clause 5.c, the Authority shall publish and maintain an up-to-date version of the Transparency Information in a format readily accessible and reusable by the general public under an open licence where applicable.

c. If, in the Authority's reasonable opinion, publication of any element of the Transparency Information would be contrary to the public interest, the Authority shall be entitled to exclude such information from publication. The Authority acknowledges that it would expect the public interest by default to be best served by publication of the Transparency Information in its entirety. Accordingly, the Authority acknowledges that it shall only exclude Transparency Information from publication in exceptional circumstances and agrees that where it decides to exclude information from publication on that basis, it will provide a clear statement to the general public explaining the categories of information that have been excluded from publication and reasons for withholding that information.

d. The Contractor shall assist and co-operate with the Authority as reasonably required to enable the Authority to publish the Transparency Information, in accordance with the principles set out above. Where the Authority publishes Transparency Information, it shall:

- (1) before publishing redact any information that would be exempt from disclosure if it was the subject of a request for information under the FOIA and/or the EIR, for the avoidance of doubt, including Sensitive Information;
- (2) taking into account the Sensitive Information set out in the purchase order, consult with the Contractor where the Authority intends to publish information which has been identified as Sensitive Information. For the avoidance of doubt the Authority, acting reasonably, shall have absolute discretion to decide what information shall be published or be exempt from disclosure in accordance with the FOIA and/or EIR; and
- (3) present information in a format that assists the general public in understanding the relevance and completeness of the information being published to ensure the public obtain a fair view on how this Contract is being performed.

## 6 Notices

a. A Notice served under the Contract shall be:

- (1) in writing in the English language;
- (2) authenticated by signature or such other method as may be agreed between the Parties;
- (3) sent for the attention of the other Party's representative, and to the address set out in the purchase order;
- (4) marked with the number of the Contract; and
- (5) delivered by hand, prepaid post (or airmail), facsimile transmission or, if agreed in the purchase order, by electronic mail.

b. Notices shall be deemed to have been received:

- (1) if delivered by hand, on the day of delivery if it is the recipient's Business Day and otherwise on the first Business Day of the recipient immediately following the day of delivery;
- (2) if sent by prepaid post, on the fourth Business Day (or the tenth Business Day in the case of airmail) after the day of posting;
- (3) if sent by facsimile or electronic means:
  - (a) if transmitted between 09:00 and 17:00 hours on a Business Day (recipient's time) on completion of receipt by the sender of verification of the transmission from the receiving instrument; or
  - (b) if transmitted at any other time, at 09:00 on the first Business Day (recipient's time) following the completion of receipt by the sender of verification of transmission from the receiving instrument.

## 7 Intellectual Property

a. The Contractor shall as its sole liability keep the Authority fully indemnified against an infringement or alleged infringement of any intellectual property rights or a claim for Crown use of a UK patent or registered design caused by the use, manufacture or supply of the Contractor Deliverables.

b. The Authority shall promptly notify the

Contractor of any infringement claim made against it relating to any Contractor Deliverable and, subject to any statutory obligation requiring the Authority to respond, shall permit the Contractor to have the right, at its sole discretion to assume, defend, settle or otherwise dispose of such claim. The Authority shall give the Contractor such assistance as it may reasonably require to dispose of the claim and will not make any statement which might be prejudicial to the settlement or defence of the claim.

c. Notwithstanding any other provisions of the Contract and for the avoidance of doubt, award of the Contract by the Authority and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949. The Contractor acknowledges that any such authorisation by the Authority under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific intellectual property involved.

#### **Notification of Intellectual Property Rights (IPR) Restrictions**

d. Where any of the Conditions listed below (1 to 3) have been added to these Conditions of the Contract as Project Specific DEFCONs at Clause 21, the Contractor warrants and confirms that all Intellectual Property Rights restrictions and associated export restrictions relating to the use or disclosure of the Contractor Deliverables that are notifiable under those Conditions, or of which the Contractor is or should reasonably be aware as at Effective Date of Contract, are disclosed in Schedule 6 (Notification of Intellectual Property Rights (IPR) Restrictions):

- (1) DEFCON 15 - including notification of any self-standing background Intellectual Property;
- (2) DEFCON 90 - including copyright material supplied under Clause 5;
- (3) DEFCON 91 - limitations of Deliverable Software under Clause 3b;

e. The Contractor shall promptly notify the Authority in writing if they become aware during the performance of the Contract of

any required additions, inaccuracies or omissions in Schedule 6.

f. Any amendment to Schedule 6 shall be made in accordance with DEFCON 503 (SC1).

#### **8 Supply of Contractor Deliverables and Quality Assurance**

a. This Contract comes into effect on the Effective Date of Contract.

b. The Contractor shall supply the Contractor Deliverables to the Authority at the Firm Price stated in the Schedule to the purchase order.

c. The Contractor shall ensure that the Contractor Deliverables:

- (1) correspond with the specification;
- (2) are of satisfactory quality (within the meaning of the Sale of Goods Act 1979, as amended) except that fitness for purpose shall be limited to the goods being fit for the particular purpose held out expressly by or made known expressly to the Contractor and in this respect the Authority relies on the Contractor's skill and judgement; and
- (3) comply with any applicable Quality Assurance Requirements specified in the purchase order.

d. The Contractor shall apply for and obtain any licences required to import any material required for the performance of the Contract in the UK. The Authority shall provide to the Contractor reasonable assistance with regard to any relevant defence or security matter arising in the application for any such licence.

#### **9 Supply of Data for Hazardous Substances, Mixtures and Articles in Contractor Deliverables**

a. Nothing in this Clause 9 shall reduce or limit any statutory duty or legal obligation of the Authority or the Contractor.

b. As soon as possible and in any event within the period specified in the purchase order (or if no such period is specified no later than one month prior to the delivery date), the Contractor shall provide to the Authority's representatives in the manner and format prescribed in the purchase

order:

- (1) confirmation as to whether or not to the best of its knowledge any of the Contractor Deliverables contain Hazardous Substances, Mixtures or Articles; and
  - (2) for each Substance, Mixture or Article supplied in meeting the criteria of classification as hazardous in accordance with the GB Classification, Labelling and Packaging (GB CLP) a UK REACH compliant Safety Data Sheet (SDS);
  - (3) where Mixtures supplied do not meet the criteria for classification as hazardous according to GB CLP but contain a hazardous Substance an SDS is to be made available on request; and
  - (4) for each Article whether supplied on its own or part of an assembly that contains a Substance on the UK REACH Authorisation List, Restriction List and / or the Candidate List of Substances of Very High Concern (SVHC) in a proportion greater than 0.1% w/w of the Article, sufficient information, available to the supplier, to allow safe use of the Article including, as a minimum, the name of that Substance at the time of supply.
- c. For substances, Mixtures or Articles that meet the criteria list in Clause 9.b above:
- (1) if the Contractor becomes aware of new information which may affect the risk management measures or new information on the hazard, the Contractor shall update the SDS/safety Information and forward it to the Authority and to the address listed in the purchase order; and
  - (2) if the Authority becomes aware of new information that might call into question the appropriateness of the risk management measures identified in the safety information supplied, shall report this information in writing to the Contractor.
- d. If the Substances, Mixtures or Articles in Contractor Deliverables are Ordnance, Munitions or Explosives (OME), in addition to the requirements of the GB CLP and UK REACH the Contractor shall comply with

hazard reporting requirements of DEF STAN 07-085 Design Requirements for Weapons and Associated Systems.

e. If the Substances, Mixtures or Articles in Contractor Deliverables, are or contain or embody a radioactive substance as defined in the Ionising Radiation Regulations SI 2017/1075, the Contractor shall additionally provide details on DEFFORM 68 of:

- (1) activity; and
- (2) the substance and form (including any isotope).

f. If the Substances, Mixtures and Articles in Contractor Deliverables have magnetic properties which emit a magnetic field, the Contractor shall additionally provide details on DEFFORM 68 of the magnetic flux density at a defined distance, for the condition in which it is packed.

g. Failure by the Contractor to comply with the requirements of this Condition shall be grounds for rejecting the affected Substances, Mixtures and Articles in Contractor Deliverables. Any withholding of information concerning hazardous Substance, Mixtures or Articles in Contractor Deliverables shall be regarded as a material breach of Contract under Clause 18 (Material Breach) for which the Authority reserves the right to require the Contractor to rectify the breach immediately at no additional cost to the Authority or to terminate the Contract in accordance with Clause 18.

h. Where delivery is made to the Defence Fulfilment Centre (DFC) and / or other Team Leidos location / building, the Contractor must comply with the Logistic Commodities and Services Transformation (LCST) Supplier Manual.

## **10 Delivery / Collection**

a. The purchase order shall specify whether the Contractor Deliverables are to be delivered to the consignee by the Contractor or collected from the consignor by the Authority.

b. Title and risk in the Contractor Deliverables shall pass from the Contractor to the Authority on delivery or on collection in accordance with Clause 10.a.

c. The Authority shall be deemed to have accepted the Contractor Deliverables within a reasonable time after title and risk has passed to the Authority unless it has rejected the Contractor Deliverables within the same period.

### **11. Marking of Contractor Deliverables**

a. Each Contractor Deliverable shall be marked in accordance with the requirements specified in the purchase order or if no such requirement is specified, the Contractor shall mark each Contractor Deliverable clearly and indelibly in accordance with the requirements of the relevant DEF-STAN 05-132 as specified in the contract or specification. In the absence of such requirements, the Contractor Deliverables shall be marked with the MOD stock reference, NATO Stock Number (NSN) or alternative reference number shown in the Contract.

b. Any marking method used shall not have a detrimental effect on the strength, serviceability or corrosion resistance of the Contractor Deliverables.

c. The marking shall include any serial numbers allocated to the Contractor Deliverable.

d. Where because of its size or nature it is not possible to mark a Contractor Deliverable with the required particulars, the required information should be included on the package or carton in which the Contractor Deliverable is packed, in accordance with Clause 12 (Packaging and Labelling (excluding Contractor Deliverables containing Ammunition or Explosives)).

### **12 Packaging and Labelling of Contractor Deliverables (Excluding Contractor Deliverables Containing Ammunition or Explosives)**

a. The Contractor shall pack or have packed the Contractor Deliverables in accordance with any requirements specified in the purchase order and Def Stan 81-041 (Part 1 and Part 6).

b. The Contractor shall establish if the Contractor Deliverables are, or contain, Dangerous Goods as defined in the

Regulations set out in this Clause 12. Any that do shall be packaged for UK or worldwide shipment by all modes of transport in accordance with the following unless otherwise specified in the Schedule to the purchase order:

(1) the Technical Instructions for the Safe Transport of Dangerous Goods by Air (ICAO), IATA Dangerous Goods Regulations;

(2) the International Maritime Dangerous Goods (IMDG) Code;

(3) the Regulations Concerning the International Carriage of Dangerous Goods by Rail (RID); and

(4) the European Agreement Concerning the International Carriage of Dangerous Goods by Road (ADR).

c. Certification markings, incorporating the UN logo, the package code and other prescribed information indicating that the package corresponds to the successfully designed type shall be marked on the packaging in accordance with the relevant regulation.

### **13 Plastic Packaging Tax**

a. The Contractor shall ensure that any PPT due in relation to this Contract is paid in accordance with the PPT Legislation.

b. The Contract Price includes any PPT that may be payable by the Contractor in relation to the Contract.

c. On reasonable notice being provided by the Authority, the Contractor shall provide and make available to the Authority details of any PPT they have paid that relates to the Contract.

d. The Contractor shall notify the Authority, in writing, in the event that there is any adjustment required to the Contract Price in accordance with section 70 of the Finance Act 2021 and, on reasonable notice being provided by the Authority, the Contractor shall provide any such information that the Authority requires in relation to any such adjustment.

e. In accordance with DEFCON 609 (SC1) the Contractor (and their sub-contractors) shall maintain all records relating to PPT and make them available to the Authority when requested on reasonable notice for

reasons related to the Contract.

f. Where the Contractor manufactures, purchases or imports into the UK any Plastic Packaging Component in relation to the Contract the Contractor shall, on reasonable notice being given, provide the Authority with such information and documentation that it requires to enable the Authority to carry out due diligence checks and satisfy itself that the Contractor has complied with the requirements of the PPT Legislation. This shall include, but is not limited to the Contractor providing:

- (1) confirmation of the tax status of any Plastic Packaging Component;
- (2) documents to confirm that PPT has been properly accounted for;
- (3) product specifications for the packaging components, including, but not limited to, the weight and composition of the products and any other product specifications that may be required; and
- (4) copies of any certifications or audits that have been obtained or conducted in relation to the provision of Plastic Packaging Components.

g. The Authority shall have the right, on providing reasonable notice, to physically inspect or conduct an audit on the Contractor, to ensure any information that has been provided in accordance with Clause 13.f above is accurate.

h. In the event the Contractor is not required to register for PPT they (and to the extent applicable, their sub-contractors) shall provide the Authority with a statement to this effect and, to the extent reasonably required by the Authority on reasonable notice, supporting evidence for that statement.

i. The Contractor shall provide, on the Authority providing reasonable notice, any information that the Authority may require from the Contractor for the Authority to comply with any obligations it may have under the PPT Legislation.

#### **14 Progress Monitoring, Meetings and Reports**

The Contractor shall attend progress meetings and deliver reports at the

frequency or times (if any) specified in the purchase order and shall ensure that its Contractor's representatives are suitably qualified to attend such meetings. Any additional meetings reasonably required shall be at no cost to the Authority.

#### **15 Payment**

a. Payment for Contractor Deliverables will be made by electronic transfer and prior to submitting any claims for payment under Clause 15b the Contractor will be required to register their details (Supplier on-boarding) on the Contracting, Purchasing and Finance (CP&F) electronic procurement tool.

b. Where the Contractor submits an invoice to the Authority in accordance with Clause 15a, the Authority will consider and verify that invoice in a timely fashion.

c. The Authority shall pay the Contractor any sums due under such an invoice no later than a period of 30 days from the date on which the Authority has determined that the invoice is valid and undisputed.

d. Where the Authority fails to comply with Clause 15b and there is undue delay in considering and verifying the invoice, the invoice shall be regarded as valid and undisputed for the purpose of Clause 15c after a reasonable time has passed.

e. The approval for payment of a valid and undisputed invoice by the Authority shall not be construed as acceptance by the Authority of the performance of the Contractor's obligations nor as a waiver of its rights and remedies under this Contract.

f. Without prejudice to any other right or remedy, the Authority reserves the right to set off any amount owing at any time from the Contractor to the Authority against any amount payable by the Authority to the Contractor under the Contract or under any other contract with the Authority, or with any other Government Department.

#### **16 Dispute Resolution**

a. The Parties will attempt in good faith to resolve any dispute or claim arising out of or relating to the Contract through negotiations between the respective representatives of the Parties having



authority to settle the matter, which attempts may include the use of any alternative dispute resolution procedure on which the Parties may agree.

b. In the event that the dispute or claim is not resolved pursuant to Clause 16.a the dispute shall be referred to arbitration and shall be governed by the Arbitration Act 1996. For the purposes of the arbitration, the arbitrator shall have the power to make provisional awards pursuant to Section 39 of the Arbitration Act 1996.

c. For the avoidance of doubt it is agreed between the Parties that the arbitration process and anything said, done or produced in or in relation to the arbitration process (including any awards) shall be confidential as between the Parties, except as may be lawfully required in judicial proceedings relating to the arbitration or otherwise. No report relating to anything said, done or produced in or in relation to the arbitration process may be made beyond the tribunal, the Parties, their legal representatives and any person necessary to the conduct of the proceedings, without the concurrence of all the Parties to the arbitration.

## **17 Termination for Corrupt Gifts**

The Authority may terminate the Contract with immediate effect, without compensation, by giving written notice to the Contractor at any time after any of the following events:

- a. where the Authority becomes aware that the Contractor, its employees, agents or any sub-contractor (or anyone acting on its behalf or any of its or their employees):
  - (1) has offered, promised or given to any Crown servant any gift or financial or other advantage of any kind as an inducement or reward;
  - (2) commits or has committed any prohibited act or any offence under the Bribery Act 2010 with or without the knowledge or authority of the Contractor in relation to this Contract or any other contract with the Crown;
  - (3) has entered into this or any other contract with the Crown in connection with which commission has been paid or has been agreed to be paid by it or

on its behalf, or to its knowledge, unless before the contract is made particulars of any such commission and of the terms and conditions of any such agreement for the payment thereof have been disclosed in writing to the Authority.

- b. In exercising its rights or remedies to terminate the Contract under Clause 17.a. the Authority shall:

- (1) act in a reasonable and proportionate manner having regard to such matters as the gravity of, and the identity of the person committing the prohibited act;
- (2) give due consideration, where appropriate, to action other than termination of the Contract, including (without being limited to):
  - (a) requiring the Contractor to procure the termination of a subcontract where the prohibited act is that of a Subcontractor or anyone acting on its or their behalf;
  - (b) requiring the Contractor to procure the dismissal of an employee (whether its own or that of a Subcontractor or anyone acting on its behalf) where the prohibited act is that of such employee.

- c. Where the Contract has been terminated under Clause 17.a. the Authority shall be entitled to purchase substitute Contractor Deliverables from elsewhere and recover from the Contractor any costs and expenses incurred by the Authority in obtaining the Contractor Deliverables in substitution from another supplier.

## **18 Material Breach**

In addition to any other rights and remedies, the Authority shall have the right to terminate the Contract (in whole or in part) with immediate effect by giving written notice to the Contractor where the Contractor is in material breach of their obligations under the Contract. Where the Authority has terminated the Contract under Clause 18 the Authority shall have the right to claim such damages as may have been sustained as a result of the Contractor's material breach of the Contract.

## 19 Insolvency

The Authority shall have the right to terminate the contract if the Contractor is declared bankrupt or goes into liquidation or administration. This is without prejudice to any other rights or remedies under this Contract.

## 20 Limitation of Contractor's Liability

a. Subject to Clause 20.b the Contractor's liability to the Authority in connection with this Contract shall be limited to £5m (five million pounds).

b. Nothing in this Contract shall operate to limit or exclude the Contractor's liability:

(1) for:

a. any liquidated damages (to the extent expressly provided for under this Contract);

b. any amount(s) which the Authority is entitled to claim, retain or withhold in relation to the Contractor's failure to perform or under-perform its obligations under this Contract, including service credits or other deductions (to the extent expressly provided for under this Contract);

c. any interest payable in relation to the late payment of any sum due and payable by the Contractor to the Authority under this Contract;

d. any amount payable by the Contractor to the Authority in relation to TUPE or pensions to the extent expressly provided for under this Contract;

(2) under Clause 7 of the Contract (Intellectual Property), and DEFCONs 91 or 638 (SC1) where specified in the contract;

(3) for death or personal injury caused by the Contractor's negligence or the negligence of any of its personnel,

agents, consultants or sub-contractors;

(4) for fraud, fraudulent misrepresentation, wilful misconduct or negligence;

(5) in relation to the termination of this Contract on the basis of abandonment by the Contractor;

(6) for breach of the terms implied by Section 2 of the Supply of Goods and Services Act 1982; or

(7) for any other liability which cannot be limited or excluded under general (including statute and common) law.

c. The rights of the Authority under this Contract are in addition to, and not exclusive of, any rights or remedies provided by general (including statute and common) law.

**21 The project specific DEFCONs and DEFCON SC variants that apply to this Contract are:**

**DEFCON 076 (SC1)** (Edn. 11/22) - Contractor's Personnel At Government Establishments

**DEFCON 503 (SC1)** (Edn. 06/22) - Formal Amendments to the Contract

**DEFCON 531 (SC1)** (Edn. 09/21) - Disclosure of Information

**DEFCON 532B** (Edn. 12/22) - Protection Of Personal Data (Where Personal Data is being processed on behalf of the Authority)

**DEFCON 534** (Edn 06/21) - Subcontracting and Prompt Payment

**DEFCON 537** (Edn 12/21) - Rights of Third Parties

**DEFCON 538** (Edn 06/02) – Severability

**DEFCON 539** (Edn 01/22) - Transparency

**DEFCON 566** (Edn 04/24) - Change of Control of Contractor

**DEFCON 606 (SC1)** (Edn 07/21) - Change and Configuration Control Procedure

**DEFCON 608** (Edn 07/21) - Access and Facilities to be Provided by the Contractor

**DEFCON 609 (SC1)** (Edn. 07/21) - Contractor's Records

**DEFCON 620 (SC1)** (Edn.06/22) - Contract Change Control Procedure

**DEFCON 656A** (Edn 08/16) - Termination for Convenience (Contracts Under £5M)

**DEFCON 658 (SC1)** (Edn. 10/22) – Cyber

**DEFCON 658 - Cyber Risk Profile - Moderate**

Note: Further to DEFCON 658 the Cyber Risk Profile of the Contract is Moderate, as defined in Def Stan 05-138. (RAR: 240718A06)

**DEFCON 660** (Edn 12/15) - Official-Sensitive Security Requirements

**22 The special conditions that apply to this Contract are:** Not Applicable

**23 The processes that apply to this Contract are:** Contract Change Control Procedure

If the Contractor wishes to propose a change, it shall serve a Contractor Change Proposal on the Authority, in accordance with the Contract Change Control Procedure defined under Defcon 620.

## General Conditions

### Third Party IPR Authorisation

#### **AUTHORISATION BY THE CROWN FOR USE OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS**

Notwithstanding any other provisions of the Contract and for the avoidance of doubt, award of the Contract by the Authority and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949. The Contractor acknowledges that any such authorisation by the Authority under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific intellectual property involved.

### **Russian and Belarusian Exclusion Condition**

1. The Contractor shall, and shall procure that their Sub-contractors shall, notify the Authority in writing as soon as they become aware that:
  - a. the Contract Deliverables and/or Services contain any Russian/Belarusian products and/or services; or
  - b. that the Contractor or any part of the Contractor's supply chain is linked to entities who are constituted or organised under the law of Russia or Belarus, or under the control (full or partial) of a Russian/Belarusian person or entity. Please note that this does not include companies:
    - (1) registered in the UK or in a country with which the UK has a relevant international agreement providing reciprocal rights of access in the relevant field of public procurement; and/or
    - (2) which have significant business operations in the UK or in a country with which the UK has a relevant international agreement providing reciprocal rights of access in the relevant field of public procurement.
2. The Contractor shall, and shall procure that their Sub-contractors shall, include in such notification (or as soon as reasonably practicable following the notification) full details of the Russian products, services and/or entities and shall provide all reasonable assistance to the Authority to understand the nature, scope and impact of any such products, services and/or entities on the provision of the Contract Deliverables and/or Services.
3. The Authority shall consider the notification and information provided by the Contractor and advise the Contractor in writing of any concerns the Authority may have and/or any action which the Authority will require the Contractor to take. The Contractor shall be required to submit a response to the concerns raised by the Authority, including any plans to mitigate those concerns, within 14 business days of receipt of the Authority's written concerns, for the Authority's consideration.
4. The Contractor shall include provisions equivalent to those set out in this clause in all relevant Sub-contracts.

**Intellectual Property Rights:** See Intellectual Property Condition 7

**Payment Terms:** See Payment Condition 15

**Special Indemnity Conditions:** Not Applicable

**Quality Assurance Conditions:** The Contractor is required to provide evidence of accreditation and/or registration to the following:

- Skills Development Scotland
- EAL Engineering Course
- Scottish Qualification Authority – Academic Course

**Purchase Order****PURCHASE ORDER****SC1A PO  
(Edn 05/24)****Contract No:** DM/00181**Contract Name:** DM Beith Apprentice Training Services 2024**Dated:** 17/10/2024

Supply the Deliverables described in the Schedule to this Purchase Order, subject to the attached MOD Terms and Conditions for Less Complex Requirements (up to the applicable procurement threshold).

<b>Contractor</b>	<b>Quality Assurance Requirement (Clause 8)</b>
Name: East Kilbride East Kilbride & District Training Association Ltd  Registered Address: East Kilbride Training Centre Law Place East Kilbride Glasgow G74 4PP	<ul style="list-style-type: none"> <li>• Skills Development Scotland</li> <li>• EAL Engineering Course</li> <li>• Scottish Qualifications Authority - Academic Course</li> </ul>

<b>Consignor (if different from Contractor's registered address)</b>	<b>Transport Instructions (Clause 10)</b>
Name:   Address:	Contract Deliverables are to be:  Delivered by the Contractor  Special Instructions: Not Applicable  Collected by the Authority: Not Applicable  Special Instructions (including consignor address if different from Contractor's registered address): Not Applicable

<b>Progress Meetings (Clause 14)</b>	<b>Progress Reports (Clause 14)</b>
The Contractor shall be required to attend the following meetings:  Subject: Refer to Statement of Requirement and Contractual Deliverables for DM/00181  Frequency: Monthly Visits/Meetings	The Contractor is required to submit the following Reports:  Subject: Refer to Statement of Requirement and Contractual Deliverables for DM/00181  1. Attendance sheets every week Monitoring, assessing,

<p>Bi-annual meetings to discuss matters of common interest regarding the training programme and provide access for an annual audit.</p> <p>Location: The Contractor shall provide the Venue, Chairman, Secretary and minutes for these meetings.</p>	<p>observing and reviewing individual apprentice progress in accordance with the apprentice levy</p> <p>2. Progress reports at least every 3 months (or by exception for poor performance or inefficiency) during the duration of individual's training and during the period of on-site training</p> <p>Method of Delivery: Via email (pdf, Microsoft word or excel)</p> <p>Delivery Address: kevin.mcgachy101@mod.gov.uk</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### Payment (Clause 15)

**Payment is to be enabled by CP&F.**

Forms and Documentation	Supply of Hazardous Deliverables (Clause 9)
<p>Forms can be obtained from the following websites:</p> <p><a href="https://www.kid.mod.uk/maincontent/business/commercial/index.htm">https://www.kid.mod.uk/maincontent/business/commercial/index.htm</a> (Registration is required).</p> <p><a href="https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement#invoice-processing">https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement#invoice-processing</a></p> <p><a href="https://www.dstan.mod.uk/">https://www.dstan.mod.uk/</a> (Registration is required).</p> <p>The MOD Forms and Documentation referred to in the Conditions are available free of charge from:</p> <p>Ministry of Defence, Forms and Pubs Commodity Management PO Box 2, Building C16, C Site Lower Arncott Bicester, OX25 1LP (Tel. 01869 256197 Fax: 01869 256824)</p> <p>Applications via email: <a href="mailto:Leidos-FormsPublications@teamleidos.mod.uk">Leidos-FormsPublications@teamleidos.mod.uk</a></p>	<p>A completed DEFFORM 68 (Hazardous and Non-Hazardous Substances, Mixture or Articles Statement) and, if applicable, UK REACH compliant Safety Data Sheet(s) (SDS) including any related information to be supplied in compliance with the Contractor's statutory duties under Clauses 9.b, and any information arising from the provisions of Clause 9 are to be provided by email with attachment(s) in Adobe PDF or MS WORD format to:</p> <p>(1) Hard copies to be sent to:</p> <p>Hazardous Stores Information System (HSIS) Spruce 2C, #1260 MOD Abbey Wood (South) Bristol, BS34 8JH</p> <p>(2) Emails to be sent to:</p> <p>b. <a href="mailto:DESTECH-QSEPEnv-HSISMulti@mod.gov.uk">DESTECH-QSEPEnv-HSISMulti@mod.gov.uk</a></p> <p>SDS which are classified above OFFICIAL including Explosive Hazard Data Sheets (EHDS) for Ordnance, Munitions or Explosives (OME) are not to be sent to HSIS and must be held by the respective Authority Delivery Team</p>

If you require this document in a different format (i.e. in a larger font) please contact the Authority's Representative (Commercial Officer), detailed below.

### Offer and Acceptance

A) The Purchase Order constitutes an offer by the Contractor to supply the Deliverables. This is open for acceptance by the Authority for 90 days from the date of signature. By signing the Purchase Order the Contractor agrees to be bound by the attached Terms and Conditions for Less Complex Requirements (Up to the applicable procurement threshold).

Name (Block Capitals):  
DAVID BELL

Position:  
General Manager & Secretary

For and on behalf of the Contractor

Authorised Signatory



Date: 14/11/2024

B) Acceptance

Name (Block Capitals): JACQUELINE BARRY

Position: Commercial Officer  
For and on behalf of the Authority

Authorised Signatory



Date: 19/12/2024

**C) Effective Date of Contract: 19/12/2024**



## **SC1A Schedules**

### **Schedule 1 - Additional Definitions of Contract**

**EAL** means the Specialist Skills Partner and Awarding Organisation for Engineering

**SDS** means Skills Development Scotland

**SQA** means Scottish Qualification Authority

## Schedule 2 – Schedule of Requirements

## SCHEDULE OF REQUIREMENTS FOR THE PROVISION OF APPRENTICE TRAINING FOR DM BEITH

Item Number	Specification	Cohort 1 (Year 1 24/25)	Cohort 1 (Year 1 24/25)	Cohort 1 (Year 3 26/27)	Option 1 Cohort 2 (Year 1 25/26)	Option 1 Cohort 2 (Year 1 26/27)	Option 1 Cohort 2 (Year 1 27/28)
1.	Provision of training, assessment and education of up-to 6 Apprentices towards successful attainment of a Level 3 Mechanical Craft Apprenticeship Programme of vocational/academic training in accordance with the Statement of Requirements (SoR) at Schedule 3.	Per apprentice £XX  Firm Total Price Ex VAT <b>£XX</b>	Per apprentice £XX  Firm Total Price Ex VAT <b>£XX</b>	Per apprentice £XX  Firm Total Price Ex VAT <b>£XX</b>	Per apprentice £XX  Firm Total Price Ex VAT <b>£XX</b>	Per apprentice £XX  Firm Total Price Ex VAT <b>£XX</b>	Per apprentice £XX  Firm Total Price Ex VAT <b>£XX</b>
2.	Registration Fee for Apprentices over the age of 20 years.	Per apprentice  £XX  Firm Total Price Ex VAT <b>£XX</b>		Per apprentice  £XX  Firm Total Price Ex VAT <b>£XX</b>	Per apprentice  £XX  Firm Total Price Ex VAT <b>£XX</b>		Per apprentice  £XX  Firm Total Price Ex VAT <b>£XX</b>

Total Firm Price Ex Vat £ for Cohort 1 & 2							£99,856.00

Item Number	Consignee Address (XY code only)

## Schedule 3 – Statement of Requirements



### DEFENCE MUNITIONS

### DM BEITH APPRENTICE TRAINING

DM/00181

### STATEMENT OF Requirement (SoR)

Version: 01

Date: 24 Jan 2024

THIS DOCUMENT IS THE PROPERTY OF  
HER BRITANNIC MAJESTY'S GOVERNMENT,  
And is issued for the information of such persons only as need.  
to know its contents in the course of their duties.  
Any person finding this document should hand it to a British  
Forces unit or to a police station for its safe return to the  
MINISTRY OF DEFENCE, D MOD SY, LONDON SW1 2HB,  
With particulars of how and where found.

THE UNAUTHORISED RETENTION OR DESTRUCTION OF THE DOCUMENT IS AN OFFENCE  
UNDER THE OFFICIAL SECRETS ACTS OF 1911–1989

DOCUMENT ISSUE STATUS:

<u>Issue Number:</u>	<u>Date of Issue:</u>
0.1	24 Jan 2024

RECORD OF AMENDMENTS:

<u>Number</u>	<u>Date</u>	<u>Reason for Change</u>	<u>Amended by</u>

## 1. Introduction

1.1. Defence Munitions ('the Authority') requires the Contractor to provide services to train, assess and educate 6 Apprentices towards successful attainment of the following qualifications over a 3 (three) year period starting from August each year. Precise timeframes shall be agreed with the Authority's Project Manager

### 1.2. Background

1.2.1. Defence Munitions (DM) Beith strips, builds, maintains, and tests several differing complex weapon systems. This activity is undertaken by trained and competent Weapon Ordnance Munitions Explosive (WOME) craft engineers either mechanically or electrically qualified, competent, and certified via deeds of engineering apprenticeship.

1.2.2. The DM Beith original craft apprenticeship scheme was closed dis-established in 2007. As a result DM Beith relied on the market for recruitment; however when attempting to recruit skilled engineers we struggled to firstly attract sufficient candidates in a competitive market and secondly the candidates we have managed to attract were generally of a poorer engineering standard than we would wish and they have very little to offer within the WOME context thus increasing the training burden for new staff.

1.2.3. As part of the business risk mitigation Director Weapons and Defence Munitions Team Leader approved a business case to re-introduce a craft apprenticeship at DM Beith to help sustain the craft and WOME skills requirement going forward. Hence in 2014 DM Beith re-commenced training engineering apprentices via a commercial contract with a local training provider.

1.2.4. Since 2014 DM Beith have recruited and qualified 6 apprentices each year using provider East Kilbride & District Group Training Association (EKGTA). We are still contracted with EKGTA through contract DM 00167 for the services required for the 2021 intake, 2022 intake and 2023 intake. The option to recruit in 2024 has now been taken up, subsequently there is now a need to provide the training services to support the training and assessing of 6 apprentices in 2024 with an option to recruit further in 2025.

1.3. The Contractor shall provide services to Defence Munitions site listed at Table 1 below.

**TABLE 1**

DM Site Name	Site Representative	Address
DM Beith	Kevin McGachy (ATM)	Defence Munitions Beith Beith North Ayrshire KA15 1JT

1.4. To support the continuation of a Craft engineering apprenticeship scheme at Defence Munitions Beith.

1.4.1. To train, assess and educate 6 (six) apprentices towards successful attainment of the following qualifications:

- SVQ Level 2 Performing Engineering Operations (to be carried out at the supplier's site)
- SVQ Level 3 in an Engineering Discipline (On the Job at DM Beith)
- All five Core Skills at SCQF Level 5 (minimum)
- An academic qualification: National Certificate in Mechanical or Electrical Engineering (to be carried out at the supplier's site)

These collectively would constitute the basic training achievements deemed appropriate to permit MoD to issue Deeds of Apprenticeship on completion.

1.4.2. Prior to the commencement of training, the supplier shall give all apprentices an induction to the training establishment, emphasising all the relevant health & safety requirements. The supplier shall adhere to all applicable health and safety legislation throughout the training period and ensure that the health and safety of the apprentices is not compromised.

1.4.3. The supplier shall provide each apprentice with a training logbook in the agreed MoD format and shall ensure that apprentices keep logbooks up to date and that each logbook entry is accurate and cross-referenced to the relevant section of the SVQ standards.

1.4.4. The supplier shall provide progress reports at least every 3 months (or by exception for poor performance or inefficiency) during the duration of individual's training and during the period of on-site training, the supplier will facilitate monthly visits/meetings with the DM Beith appointed representatives.

1.4.5. The supplier will support bi-annual meetings to discuss matters of common interest regarding the training programme and provide access for an annual audit.

1.4.6. The supplier will deliver the minimum of 40 weeks training to achieve an SVQ level 2, a National Certificate in Mechanical or Electrical Engineering and achievement of the five Core Skills at Intermediate 1 and pay appropriate college fees.

1.4.7. The supplier will be responsible for drawing down additional funding from the Skills Development Scotland to cover additional costs including registration, certification, monitoring, assessment, and verification.

1.4.8. MoD would expect the supplier to pass to MoD any refund of the percentage of the output-based funding paid to the supplier upon successful completion of all aspects of the Apprentice programme.

- 1.5. This Contract requirement has been identified by the Authority to continue DM Beith's established apprentice scheme. This recruitment and training activity will then enable recruitment of suitably qualified experience personnel to work within the engineering roles within the Engineering/WOME sector of Defence Munitions.
- 1.6. The duration of this Contract shall be for 3 years from the effective date of contract as detailed in Part C of the Purchase Order. With one Option year for an intake in 2025, which if invoked are to be raised in accordance with DEFCON 503 (Formal Amendments to Contract).
- 1.7. In the event that an apprentice resigns or leaves the apprenticeship, the Authority reserves the right to amend the contract to reflect the price decrease and total quantity of apprentices. The price reduction will be the total per individual apprentice for any training elements which have not yet commenced at the point of resignation/leaving. Any reduction in the total firm price of the contract will be raised in accordance with DEFCON 503 (Formal Amendments to Contract).

## **2. Core Service**

- 2.1. The scope of this Contract requirement will cover the below core services at the sites listed at Table 1 unless specified below.
  - 2.1.1 SVQ Level 2 Performing Engineering Operations (at the supplier's site)
  - 2.1.2 SVQ Level 3 in an Engineering Discipline (On the Job at DM Beith)
  - 2.1.3 All five Core Skills at SCQF Level 5 (minimum)
  - 2.1.4 An academic qualification: National Certificate in Mechanical or Electrical Engineering (to be carried out at the supplier's site).

## **Schedule 4 - Deliverables**

### **Deliverables Note**

This matrix is intended to provide an overview of the parties' contractual obligations to assist with contract management. It does not form part of the contract and should not be relied upon to aid interpretation of the contract. In the event of any conflict, inconsistency or discrepancy between this matrix and the contract, the terms of the contract shall take precedence.



## Negotiation Deliverables

Name	Description	Date	Responsible Party
None	N/A	N/A	N/A

## Buyer Contractual Deliverables

Name	Description	Due	Responsible Party
Transparency Condition 5.b	Redact documents prior to publishing in line with contract.		Buyer Organization
Termination Condition 16, 17, 18	Written notice of Termination due to corrupt Gifts as stipulated in the contract		Buyer Organization
Notification of Claim Condition 7.b	Notify contractor of any third party claim and assist the contractor to dispose of said claim		Buyer Organization
Import Licences Condition 8.d	Assist application for licences that are defence/security related		Buyer Organization

## Supplier Contractual Deliverables

Name	Description	Due	Responsible Party
Payment Condition 14.c	Payment		Supplier Organization
Contract Planning and Administration - Arrange In House Contract Initiation Meeting (reminder)	To call an initial Internal only meeting to ensure that all key MOD players understand the contract, e.g. they know: the contract scope and operation; their role & authority in the contract; the specific obligations they are responsible for; high-risk areas; performance evaluation; and what to do in response to events/problems that may arise and if changes are needed.		Supplier Organization
Obligation DEFCON 91 (Edn 06/21) Clause - 5b - Software as required	A copy of the Software as is required for performance of obligations to be retained.		Supplier Organization
Obligation DEFCON 117 (Edn 07/21) Clause - 3a - Technical Data to Codification Authority or representative	Provision of Technical Data to the Codification Authority or the Authority's Agent specified by the Codification Authority.		Supplier Organization
Obligation DEFCON 21 (Edn 06/21) Clause - 3a - Maintenance of Deliverables (reminder)	To maintain at least one copy of all deliverable information to which DEFCON 21 applies during the period of the Contract and for at least two years after the Contract, or period as may be specified in the contract.		Supplier Organization
Import Licences Condition 8.d	Apply for and obtain all necessary licences		Supplier Organization
Marking of Hazardous Deliverables Condition 9.b	Ensure packaging is marked in accordance with the contract		Supplier Organization
Contract Data Sheet Condition 9.c	provide a Safety Data Sheet in respect of each Dangerous/Hazardous Material or		Supplier Organization

	substance supplied or deliverable containing such.		
Marking of Articles Condition 11	Articles to be marked in accordance with the contract.		Supplier Organization
Progress Meetings Condition 13	Attendance at progress meetings in accordance with the contract		Supplier Organization
Payment Condition 14.b	Submission of Invoices		Supplier Organization

### Contractual Deliverables for DM/00181

Name	Description	Due
Statement of Requirement 1.4.2	The supplier shall give all apprentices an induction to the training establishment, emphasising all the relevant health & safety requirements.	Prior to the commencement of training
Statement of Requirement 1.4.3	The supplier shall provide each apprentice with a training logbook in the agreed MoD format	Prior to the commencement of training
Statement of Requirement 1.4.3	The Supplier shall ensure that apprentices keep logbooks up to date and that each logbook entry is accurate and cross-referenced to the relevant section of the SVQ standards.	Duration of Contract
Statement of Requirement 1.4.4	The supplier shall provide progress reports at least every 3 months (or by exception for poor performance or inefficiency) during the duration of individual's training and during the period of on-site training	Every 3 months
Statement of Requirement 1.4.4	The supplier will facilitate monthly visits/meetings with the DM Beith appointed representatives	Every Month
Statement of Requirement 1.4.5	The supplier will support bi-annual meetings to discuss matters of common interest regarding the training programme	Bi-Annual
Statement of Requirement 1.4.6	The supplier will deliver the minimum of 40 weeks training to achieve an SVQ level 2, a National Certificate in Mechanical or Electrical Engineering and achievement of the five Core Skills at Intermediate 1 and pay appropriate college fees.	Duration of contract
Statement of Requirement 1.4.7	The supplier will be responsible for drawing down additional funding from the Skills Development Scotland to cover additional costs including registration, certification, monitoring, assessment, and verification.	As required
Statement of Requirement 1.4.8	MoD would expect the supplier to pass to MoD any refund of the percentage of the output-based funding paid to the supplier upon successful completion of all aspects of the Apprentice programme.	As required
Purchase Order	The Contractor shall submit Attendance Sheets to monitor, assess, observe and review individual apprentice progress in accordance with the apprentice levy	Weekly (Each Friday by close of play from the Start date of the Training Programme)
Purchase Order	A completed DEFFORM 68 (Hazardous and Non-Hazardous Substances, Mixture or Articles Statement) to be provided	Contract Award

**Schedule 5 – Milestone Payment Plan****MILESTONE PAYMENT PLAN FOR THE PROVISION OF APPRENTICE TRAINING FOR DM  
BEITH**

<b>Item No.</b>	<b>Description</b>	<b>Date Due</b>	<b>Firm Price (Ex VAT) (£)</b>
1	Year 1 NC in Engineered Systems (Mechanical/Electrical)	31 July 2025	£XX
2	Over 20's Registration Fee	31 July 2025	£XX
3	Year 2 Foundation Training SVQ L2	31 July 2026	£XX
4	Year 2 SVQ L3 Monitoring and Assessment (1 <sup>st</sup> instalment)	31 July 2026	£XX
5	Year 3 SVQ L3 Monitoring and Assessment (2 <sup>nd</sup> instalment)	31 July 2027	£XX
6	Over 20's SVQ L3 Additional Costs	31 July 2027	£XX
7	Funding Rebate (only upon successful completion of Apprenticeship)		

**Schedule 6 - Notification of IPR Restrictions (iaw Clause 7)**

**DEFFORM 711**

DEFFORM 711 (Edn 11/22)

**Ministry of Defence**

**DEFFORM 711 – NOTIFICATION OF INTELLECTUAL PROPERTY RIGHTS (IPR)  
RESTRICTIONS**

**DEFFORM 711 - PART A – Notification of IPR Restrictions**

NOT USED

**DEFFORM 711 - PART B – System / Product Breakdown Structure (PBS)**

NOT USED

## Schedule 7 – Cyber Implementation Plan

**CYBER IMPLEMENTATION PLAN****MODERATE CYBER RISK PROFILE****Part 1: Assurance Controls and Evidence Completed by Industry**

Organisation Name	East Kilbride & District Engineering Group Training Association Ltd	
Contact Name	David Bell	
Contact Email	david.bell@ekgta.com	
Contract Name	712133450-A - DM/00181 - DM Beith Apprentice Training Services 2024	
Cyber Risk Profile		Moderate
Risk Assessment Reference (RAR)	240718A06	
Supplier Assurance Questionnaire (SAQ) code (If known)	591026107	
Controls not met (paste from DCPD response email)	VL01, L09	
Controls are ordered by security category:		
Security Governance	L01, L02, L03, M01, M02	
Security Culture and Awareness	L04, L05, L06, M03	
Information Asset Security	L07, L08, M04, M05, M06, M07	
Info-Cyber Systems Security	VL01, L09, L10, L11, L12, L13, M08, M09, M10, M11, M12, M13, M14	
Personnel Security	L14, L15, L16, M15, M16, M17	
Security Incident Management	L17	

**Only answer for controls "not met".**

**SAQ returns with "Not met" can be submitted providing the CIP covers those controls.**

DEFSTAN 05 -138

DEFCON CONTROLS (High)	Equivalent standard / controls or comment
<b>Security Governance</b>	
<b>L.01</b> Define and implement an information security policy, related processes and procedures.	
<b>L.02</b> Define and assign information security relevant roles and responsibilities.	
<b>L.03</b> Define and implement a policy which addresses information security risks within supplier relationships.	
<b>M.01</b> Define and implement a policy which provides for regular, formal information security related reporting.	
<b>M.02</b> Define and implement a repeatable risk assessment process.	

**Security Culture and Awareness**

<b>L.04</b> Define and implement a policy which ensures all functions have sufficient and appropriately qualified resources to manage the establishment, implementation and maintenance of information security.	
<b>L.05</b> Define employee (including contractor) responsibilities for information security.	
<b>L.06</b> Define and implement a policy to provide employees and contractors with information security training.	
<b>M.03</b> Define and implement a repeatable risk assessment process.	
<b>Information Asset Security</b>	
<b>L.07</b> Define and implement a policy for ensuring sensitive information is clearly identified.	
<b>M.04 / M04a / M04b</b> Define and implement a policy for storing, accessing, and handling sensitive information securely.	
<b>M.05</b> Define and implement a policy for data loss prevention.	
<b>M.06</b> Define, implement, and test a policy for regular off-line back-up of data off-site.	
<b>L.08</b> Define and implement a policy to control access to information and information processing facilities.	
<b>M.07</b> Ensure the organisation has identified asset owners and asset owners control access to their assets.	
<b>Info-Cyber Systems Security</b>	
<b>VL.01</b> Maintain annually renewed Cyber Essentials Certification.	We have implemented a number of suggestions from our cyber security managed service provider and are in the process of gaining certification.
<b>L.09</b> Maintain annually renewed Cyber Essentials Scheme Plus Certification.	We have implemented a number of suggestions from our cyber security managed service provider and are in the process of gaining certification.

<b>L.10</b> Define and implement a policy to control the exchanging of information via removable media.	
<b>L.11</b> Record and maintain the scope and configuration of the information technology estate.	

<b>M.08</b> Define and implement a policy to assess vulnerabilities identified for which there are no countermeasures (e.g. a patch) available, undertake risk assessment and management.	
<b>M.09</b> Undertake administration access over secure protocols, using multi-factor authentication.	
<b>M.10</b> Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.	
<b>L.12</b> Define and implement a policy to manage the access rights of user accounts.	
<b>M.11</b> Define and implement a policy to monitor user account usage and to manage changes of access rights.	
<b>M.12</b> Define and implement a policy to control remote access to networks and systems.	
<b>L.13</b> Define and implement a policy to maintain the confidentiality of passwords.	
<b>M.13</b> Define and implement a policy to control the use of authorised software.	
<b>M.14</b> Define and implement a policy to control the flow of information through network borders.	
<b>Personnel Security</b>	
<b>L.14</b> Define and implement a policy for verifying an individual's credentials prior to employment.	

<b>M.15</b> Define and implement a policy for applying security vetting checks to employees	
<b>L.15</b> Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.	
<b>L.16</b> Define and implement a disciplinary process to take action against employees who violate information security policies or procedures	
<b>M.16</b> Undertake personnel risk assessments for all employees and contractors and ensure those with specific responsibilities for information security have sufficient appropriate qualifications and appropriate levels of appropriate experience	
<b>M.17</b> Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.	
<b>Security Incident Management</b>	
<b>L.17</b> Define and implement an incident management policy, which must include detection, resolution, and recovery.	

Anticipated Date of Compliance	Comment
28/03/2025	Enquiries have been made to join the Cyber Essentials scheme and these will be implemented by end March 2025



**Personal Data Particulars****DEFFORM 532**

Edn 10/19

.....

This Form forms part of the Contract and must be completed and attached to each Contract containing DEFCON 532B.

<b>Data Controller</b>	<p>The Data Controller is the Secretary of State for Defence (the Authority).</p> <p>The Personal Data will be provided by:</p> <p><i>DM Beith Apprentice Scheme</i></p> <p><i>Kevin McGachy</i></p> <p><a href="mailto:Kevin.McGachy101@mod.gov.uk">Kevin.McGachy101@mod.gov.uk</a></p> <p><i>01505 504581 x 4511</i></p>
<b>Data Processor</b>	<p>The Data Processor is the Contractor.</p> <p>The Personal Data will be processed at:</p> <p><i>East Kilbride Group Training Association</i></p> <p><i>3 Law Place</i></p> <p><i>East Kilbride</i></p> <p><i>G74 4PP</i></p> <p><i>David Bell</i></p> <p><a href="mailto:David.bell@ekgta.com">David.bell@ekgta.com</a></p> <p><i>01335 229985</i></p>
<b>Data Subjects</b>	<p>The Personal Data to be processed under the Contract concern the following Data Subjects or categories of Data Subjects:</p> <p><i>Staff/Students enrolled on the Defence Munitions Apprentice Schemes</i></p>
<b>Categories of Data</b>	<p>The Personal Data to be processed under the Contract concern the following categories of data: <i>[please specify]</i></p> <p><i>Name, Date of Birth, Address, Telephone Number, Medical Records, National Insurance Number and Awarding Bodies Candidate Number</i></p>
<b>Special Categories of data (if appropriate)</b>	<p>The Personal Data to be processed under the Contract concern the following Special Categories of data: <i>Not Applicable</i></p>
<b>Subject matter of the processing</b>	<p>The processing activities to be performed under the contract are</p>

	<p>as follows:</p> <p><i>The processing of information will be in the form of recruitment, enrolment, registration onto the scheme and awarding bodies and the assessment/review and awarding of the standards and qualifications recognised as a national standard.</i></p>
<b>Nature and the purposes of the Processing</b>	<p>The Personal Data to be processed under the Contract will be processed as follows: <i>[please specify]</i></p> <p><i>Contractors' collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, only relating to the processing noted for registration, review and awarding and all erasure or destruction of data (whether by automated means or not)</i></p>
<b>Technical and organisational measures</b>	<p>The following technical and organisational measures to safeguard the Personal Data are required for the performance of this Contract:</p> <p><i>Required in accordance with the Cyber Risk Profile moderate assessment to the Contract, as detailed in Annex A to <a href="#">Def Stan 05-138</a>.</i></p>
<b>Instructions for disposal of Personal Data</b>	<p>The disposal instructions for the Personal Data to be processed under the Contract are as follows (where Disposal Instructions are available at the commencement of Contract):</p> <p><i>Erasure or destruction of data (whether by automated means or not) etc shall be completed as soon as the information is no longer required for the purpose of the process or within 12 months of the apprenticeship end date.</i></p>
<b>Date from which Personal Data is to be processed</b>	<p>Where the date from which the Personal Data will be processed is different from the Contract commencement date this should be specified here: <i>04 April 2024</i></p>

The capitalised terms used in this form shall have the same meanings as in the General Data Protection Regulations.

**DEFFORM 111****DEFFORM 111****Appendix - Addresses and Other Information****1. Commercial Officer**

Name: Jacqueline Barry

Address: DE&S, NH4, #4110 Fir 3B, Bristol, BS34 8JH

Email: Jacqueline.Barry111@mod.gov.uk

**2. Project Manager, Equipment Support Manager or PT Leader** (from whom technical information is available)

Name: Kevin McGachy

Address: DE&S, XX Building, Beith, KA15 1JT

Email: Kevin.McGachy101@mod.gov.uk ☎☎ 01505 504581 x 4511

**3. Packaging Design Authority Organisation & point of contact:**

(Where no address is shown please contact the Project Team in Box 2)

☎☎

**4. (a) Supply / Support Management Branch or Order Manager:**

Branch/Name:

☎☎

(b) U.I.N.

**5. Drawings/Specifications are available from****6. Intentionally Blank****7. Quality Assurance Representative: XX**

**8. AQAPS and DEF STANs** are available from UK Defence Standardization, for access to the documents and details of the helpdesk visit <http://dstan.uwh.diif.r.mil.uk/> [intranet] or <https://www.dstan.mod.uk/> [extranet, registration needed].

**9. Consignment Instructions** The items are to be consigned as follows:**10. Transport.** The appropriate Ministry of Defence Transport Offices are:

**A. DSCOM**, DE&S, DSCOM, MoD Abbey Wood, Cedar 3c, Mail Point 3351, BRISTOL BS34 8JH  
Air Freight Centre

IMPORTS ☎☎ 030 679 81113 / 81114 Fax 0117 913 8943

EXPORTS ☎☎ 030 679 81113 / 81114 Fax 0117 913 8943

Surface Freight Centre

IMPORTS ☎☎ 030 679 81129 / 81133 / 81138 Fax 0117 913 8946

EXPORTS ☎☎ 030 679 81129 / 81133 / 81138 Fax 0117 913 8946

**B. JSCS**

JSCS Helpdesk No. 01869 256052 (select option 2, then option 3)

JSCS Fax No. 01869 256837

[www.freightcollection.com](http://www.freightcollection.com)

### **11. The Invoice Paying Authority**

Ministry of Defence, DBS Finance, Walker House, Exchange Flags Liverpool, L2 3YL

☎ 0151-242-2000 Fax: 0151-242-2809

**Website is:** <https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement#invoice-processing>

### **12. Forms and Documentation are available through \*:**

Ministry of Defence, Forms and Pubs Commodity Management PO Box 2, Building C16, C Site, Lower Arncott, Bicester, OX25 1LP (Tel. 01869 256197 Fax: 01869 256824)

**Applications via fax or email:** [Leidos-FormsPublications@teamleidos.mod.uk](mailto:Leidos-FormsPublications@teamleidos.mod.uk)

### **\* NOTE**

**1. Many DEFCONs and DEFFORMs** can be obtained from the MOD Internet Site:

<https://www.kid.mod.uk/maincontent/business/commercial/index.htm>

**2. If the required forms or documentation are not available on the MOD Internet site requests should be submitted through the Commercial Officer named in Section 1.**



Ministry  
of Defence



Kevin McGachy  
Project Manager

[kevin.mcgachy101@mod.gov.uk](mailto:kevin.mcgachy101@mod.gov.uk)

01505 504581 Ext 4511

Defence Equipment & Support  
Defence Munitions Beith  
Bld 250  
Beith  
Ayrshire  
KA15 1JT

17/10/2024

Our Reference:

DM/00181

Personal Data Aspects Letter (PDAL)

For the personal attention of:  
The Contractor's Data Controller

---

Dear Sir or Madam,

**PERSONAL DATA ASPECTS LETTER FOR CONTRACTS INVOLVING THE HANDLING OF  
OFFICIAL SENSITIVE PERSONAL DATA**

**TENDER / CONTRACT NO AND SUBJECT – DM Beith Apprentice Training 2024 – DM/00181**

1. On behalf of the Secretary of State for Defence, I hereby give you notice that the Privacy Impact Assessment conducted has identified that this contract involves the requirement to handle UK MOD personal data. This data is subject to the provisions of the Data Protection Act 2018,<sup>1</sup> the Data Handling Review,<sup>2</sup> and the GovS 007 Security.<sup>3</sup> Your attention is also drawn to the specific aspects of personal data handling set out in Industry Security Notices which must be fully implemented.

2. Will you please confirm that:

**a.** This definition of the personal data aspects of the above contract has been brought to the attention of the person directly responsible for the protection of data in this contract.

**b.** The definition is fully understood.

**c.** Measures can, and will, be taken to protect the personal data.

**d.** Any problems in meeting these requirements will be notified to MOD immediately.

Yours faithfully

Kevin McGachy

Project Manager Copy to:

CIO-Advisor

---

<sup>1</sup> <https://www.gov.uk/data-protection>

<sup>2</sup> <https://www.gov.uk/government/publications/data-handling-procedures-in-government>

**DEFFORM 68**  
(Edn 09/22)

## **Hazardous and Non Hazardous Substances, Mixtures or Articles Statement by the Contractor**

Contract Number: 712133450-A – DM/00181

Contract Title: DM Beith Training Services 2024

Contractor: East Kilbride & District Engineering Group Training Association Ltd

Date of Contract: 19/12/2024

\* To the best of our knowledge there are no hazardous Substances, Mixtures or Articles to be supplied. ☒; or

\* To the best of our knowledge the hazards associated with Substances, Mixtures or Articles to be supplied under the Contract are identified in the Safety Data Sheets or UK REACH Article 33 Communication attached in accordance with either:

DEFCON 68 ☐; or

Condition 9 of Standardised Contract 1A/B Conditions ☐.

Contractor's Signature: 

Name: David Bell

Job Title: General Manager & Company Secretary

Date: 14/11/2024

\* check box (☒) as appropriate

---

### **To be completed by the Authority**

DMC:

NATO Stock Number:

Contact Name:

Contact Address:

Contact Phone Number:

Contact Email Address:

Copy to be forwarded to:

Hazardous Stores Information System (HSIS)  
Spruce 2C, #1260  
MOD Abbey Wood (South)  
Bristol, BS34 8JH

Email: [DESEngSfty-QSEPSEP-HSISMulti@mod.gov.uk](mailto:DESEngSfty-QSEPSEP-HSISMulti@mod.gov.uk)

## The Statement Relating To Good Standing

**Contract Title:** DM Beith Apprentice Training Services 2024

**Contract Number:** DM/00181

1. We confirm, to the best of our knowledge and belief, that East Kilbride & District Group Training Association Limited including their directors or any other person who has powers of representation, decision or control or is a member of the administrative, management or supervisory body of East Kilbride & District Group Training Association Limited have not been convicted of any of the following offences within the past 5 years:
  - a. conspiracy within the meaning of section 1 or 1A of the Criminal Law Act 1977 or article 9 or 9A of the Criminal Attempts and Conspiracy (Northern Ireland) Order 1983 where that conspiracy relates to participation in a criminal organisation as defined in Article 2 of Council Framework Decision 2008/841/JHA;
  - b. corruption within the meaning of section 1(2) of the Public Bodies Corrupt Practices Act 1889 or section 1 of the Prevention of Corruption Act 1906;
  - c. common law offence of bribery;
  - d. bribery within the meaning of section 1,2 or 6 of the Bribery Act 2010; or section 113 of the Representation of the People Act 1983;
  - e. any offence listed: (1) in section 41 of the Counter Terrorism Act 2008; or (2) in Schedule 2 to that Act where the court has determined that there is a terrorist connection;
  - f. any offence under sections 44 to 46 of the Serious Crime Act 2007 which relates to an offence covered by (e) above;
  - g. money laundering within the meaning of section 340(11) and 415 of the Proceeds of Crime Act 2002;
  - h. an offence in connection with the proceeds of criminal conduct within the meaning of section 93A, 93B, or 93C of the Criminal Justice Act 1988 or article 45, 46 or 47 of the Proceeds of Crime (Northern Ireland) Order 1996;
  - i. an offence under section 4 of the Asylum and Immigration (Treatment of Claimants etc) Act 2004;
  - j. an offence under section 59A of the Sexual Offences Act 2003;
  - k. an offence under section 71 of the Coroners and Justice Act 2009;
  - l. an offence in connection with the proceeds of drug trafficking within the meaning of section 49, 50 or 51 of the Drug Trafficking Act 1994; or
  - m. an offence under section 2 or 4 of the Modern Slavery Act 2015;
  - n. any other offence within the meaning of Article 57(1)(a), (b), (d), (e), or (f) of Public Contracts Directive – (1) as defined by the law of any jurisdiction outside England and Wales and Northern Ireland: or (2) created in the law of England and Wales or Northern Ireland after the day on which these Regulations were made;



o. any breach of their obligations relating to the payment of taxes or social security contributions where the breach has been established by a judicial or administrative decision having final and binding effect in accordance with the legal provisions of the country in which they are established or with those of any jurisdictions of the United Kingdom.

2. East Kilbride & District Group Training Association Limited further confirms to the best of our knowledge and belief that within the last 3 years they:

a. have fulfilled their obligations relating to the payment of taxes and social security contributions of the country in which they are established or with those of any jurisdictions of the United Kingdom;

b. are not bankrupt or are not the subject of insolvency or winding-up proceedings, where their assets are being administered by a liquidator or by the court, where they are in an agreement with creditors, where their business activities are suspended or they are in any analogous situation arising from a similar procedure under the laws and regulations of any State;

c. have not committed an act of grave professional misconduct, which renders their integrity questionable;

d. have not entered into agreements with other suppliers aimed at distorting competition;

e. are not subject to a conflict of interest within the meaning of regulation 24;

f. have not been involved in the preparation of this procurement procedure which would result in distortion of competition which could not be remedied by other, less intrusive, measures other than exclusion from this procedure;

g. have not had a contract terminated, damages or other comparable sanctions taken as a result of significant or persistent deficiencies in the performance of a substantive requirement under a prior public contract, a prior contract, or a prior concession contract as defined by the Concession Contracts Regulations 2016;

h. are not guilty of serious misrepresentation in providing any information required by this statement.

i. have not unduly influenced the decision-making process of the Authority or obtained confidential information that may confer upon it undue advantages in the procurement procedure;


j. in relation to procedures for the award of a public services contract, are licensed in the relevant State in which they are established or are a member of an organisation in that relevant State where the law of that relevant State prohibits the provision of the services to be provided under the contract by a person who is not so licensed or who is not such a member;

k. have fulfilled their obligations in the fields of environmental, social and labour law established by national law, collective agreements or by the international environmental, social and labour law provisions listed in the Public Contracts Directive as amended from time to time (as listed in PPN 03/23 Annex D).

3. East Kilbride & District Group Training Association Limited confirms they, or any part(s) of their intended supply chain is / are not linked to entities who are constituted or organised under the law of Russia or Belarus or under the control (full or partial) of a Russian / Belarusian person or entity (see Candidate Note below).

I confirm that to the best of my knowledge my declaration is correct. I understand that the contracting authority will use the information in the selection process to assess my organisation's

suitability to be invited to participate further in this procurement, and I am signing on behalf of my organisation. I understand that the Authority may reject my submission if there is a failure to provide a declaration or if I provide false or misleading information.

Organisation's name	East Kilbride & District Engineering Group Training Association Ltd
Signed (By Director of the Organisation or equivalent)	
Name	David Bell
Position	General Manager & Company Secretary
Date	14/11/2024



Our reference: DM/00181

Your reference:

Date: 17/10/2024

For the Personal Attention of the  
Contractors Data Controller

Dear Sir/Madam,

**SECURITY ASPECTS LETTER FOR: Apprentice Training Contract Award, Defence Munitions Beith**

1. On behalf of the Secretary of State for Defence, I hereby give you notice of the information or assets connected with, or arising from, the referenced Contract that constitute classified material.
2. Aspects that constitute OFFICIAL-SENSITIVE <sup>1</sup>for the purpose of DEFCON 660 are specified separately and not for publication.
3. Information about this contract must not, without the approval of the Authority, be published or communicated further to anyone except where necessary for the execution of the contract.
4. For the solution that is being used to deliver the contracted service, whether it is an asset being delivered to the Authority, an asset owned or leased by the supplier or an asset where DE&S is not the sole user, suppliers must follow the DE&S Secure by Design (SbD) process as guided by the DE&S Delivery Team. Consequently, the supplier must assist DE&S by providing them with the requested information to support the SbD assurance process.
5. Your attention is drawn to the requirements of the 'Security Conditions' at Annexes B through D, and the provisions of the Official Secrets Act 1989 and National Security Act 2023. In particular you should take all reasonable steps to make sure that all individuals employed on any work in connection with this Contract have notice of the above specified aspects and that the aforementioned statutory provisions apply to them and will continue to apply after completion or earlier termination of the contract.
6. The enclosed Security Conditions at Annex C outline the principal measures required to safeguard OFFICIAL-SENSITIVE information are provided to enable you to apply the required degree of protection.
7. If any security incidents occur to classified information regarding this contract, then it shall be reported in accordance the requirements laid down in Annex C.
8. The 'Need to Know' security principle is to be enforced rigorously at all times with regards to all project material (e.g., documentation, drawings, conversation).
9. The rules and regulations laid down within the following DEFCONs are to be strictly adhered to:

---

<sup>1</sup> See Technical Grading Guides for greater clarification

- a. DEFCON 76 Contractor's Personnel at Government Establishments
- b. DEFCON 531 Disclosure of Information
- c. DEFCON 658 Cyber
- d. DEFCON 660 Official-Sensitive Security requirements.

10. Will you please confirm that:

- a. This definition of the classified aspects of the referenced Contract has been brought to the attention of the person directly responsible for security of classified material.
- b. The definition is understood and that the requirements of this Security Aspects Letter and the UK Security Conditions will be complied with using the Acceptance letter at Annex A.
- c. Measures can, and will, be taken to safeguard the classified aspects identified herein in accordance with applicable national laws and regulations. [The requirement and obligations set out above and in any contractual document can and will be met and that the classified information shall be protected in accordance with applicable national laws and regulations.]
- d. All employees of the company who will have access to classified information have either signed the OSA Declaration Form in duplicate and one copy is retained by the Company Security Officer or have otherwise been informed that the provisions of the OSA apply to all classified information and assets associated with this contract.

11. If you have any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will you please let me know immediately.

12. The Contractor shall ensure that all individuals (contractors, sub-contractors and agency personnel) working on Defence Contracts must apply the requirements of HMG Baseline Personnel Security Standard (Minimum BPSS)[1]. The contracting company should be able to demonstrate that the checks have been carried out satisfactorily and are in place and that such checks may be audited, and spot checked by the contracting organisation.

13. Any access to classified information or assets on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Officer in accordance with DEFCON 76.

Yours faithfully,

The following Annexes provide key SAL addition information for guidance/reference/acknowledgment:

A. Acceptance of DE&S Security Aspects Letter (SAL.

---

[1] [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/677553/HMG\\_Baseline\\_Personnel\\_Security\\_Standard.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/677553/HMG_Baseline_Personnel_Security_Standard.pdf)

- B. [Technical Grading Guide - Redacted](#)
- C. [OFFICIAL-SENSITIVE Security Condition for UK Contracts.](#)
- D. [Official Secrets Act section 2.](#)
- E. [DEFCON 76 Contractor's Personnel at Government Establishments.](#)
- F. [DEFCON 531 Disclosure of Information.](#)
- G. [DEFCON 658 Cyber](#)
- H. [DEFCON 660 Official-Sensitive Security requirements.](#)
- I. [Apprentice Training Contract Beith- SAL Acknowledgment Sheet for Employees or Subcontracts](#)

Final SAL Copy to be sent to:

Redacted

**Annex A to Apprentice Training Contract Beith**  
**Dated: 17/10/2024**

## **ACCEPTANCE OF SECURITY ASPECTS LETTER (SAL)**

1. Receipt of the above SAL is acknowledged. On behalf of the contractor, I confirm that:

a. The content within Annexes B to H, together with all the security requirements described within this SAL, is understood. This content is to be briefed to all personnel who will be working on this contract / task and all sub-contractors, who require access to Project Information.

b. The classified information, within Annexes B to H, has been brought to the attention of the person directly responsible for the security of this contract. This will include supplying suitable SALs and references to your sub-contractors.

c. Copies of all sub-contractor SALs will be sent to the undersigned or their representative.

Measures will be taken to safeguard the Controlled Material and/or OFFICIAL-SENSITIVE / OFFICIAL Matter in line with policies and procedures outlined within Annex C of this document.

d. Individuals 'need to know' and access requirements in relation to **Apprentice Training Contract Beith**, and are strictly role-based, and therefore, automatically rescinded on job change or departure.

e. All conditions and requirements above in this SAL will be complied with.

Signed<sup>2</sup> 

Date 14/11/2024

Name: David Bell

Job Title: General Manager & Company Secretary

---

<sup>2</sup> To be signed by the Project Director only. Remaining project staff are to sign Annex I.

**TECHNICAL GRADING GUIDE FOR OFFICIAL SENSITIVE INFORMATION**

**Not provided for contract publishing**

## **ANNEX C: UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS<sup>3</sup>**

### **Purpose**

1. This document provides guidance for Defence Suppliers where classified material provided to or generated by the Defence Supplier is graded UK OFFICIAL or UK OFFICIAL-SENSITIVE. Where the measures requested below cannot be achieved or are not fully understood, further advice should be sought from the UK Designated Security Authority (Email: [COO-DSR-IIPCSy@mod.gov.uk](mailto:COO-DSR-IIPCSy@mod.gov.uk)).

### **Definitions**

2. The term "Authority" for the purposes of this Annex means the UK MOD Contracting Authority.
3. The term "Classified Material" for the purposes of this Annex means classified information and assets.

### **Security Grading**

4. The SENSITIVE marking is used to denote UK OFFICIAL material that is of a particular sensitivity and where there is a need to reinforce the 'need to know'. The Security Aspects Letter, issued by the Authority shall define the UK OFFICIAL-SENSITIVE material that is provided to the Defence Supplier, or which is to be developed by it, under this Contract. The Defence Supplier shall mark all UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security grading. The Defence Supplier is not required to mark documents graded UK OFFICIAL unless they are transmitted overseas or generated by a Defence Supplier based outside the UK in a third-party country.

### **Security Conditions**

5. The Defence Supplier shall take all reasonable steps to adhere to the provisions specified in the Contract or listed in this Annex. The Defence Supplier shall make sure that all individuals employed on any work in connection with the Contract have notice that these provisions apply to them and shall continue so to apply after the completion or earlier termination of the Contract.
6. Where a Defence Supplier is based outside the UK in a third-party country the national rules and regulations of the third-party country take precedence over these conditions only if the third-party country has an extant bilateral security agreement or arrangement with the UK.
7. The Authority shall state the data retention periods to allow the Defence Supplier to produce a data management policy.

---

<sup>3</sup> JSP 440 Leaflet 6a Annex B – issued April 24



8. If you are a Defence Supplier located in the UK, your attention is also drawn to the provisions of the Official Secrets Act 1989 and the National Security Act 2023.

### **Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Classified Material**

9. The Defence Supplier shall protect UK OFFICIAL and UK OFFICIAL-SENSITIVE material provided to or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Defence Supplier shall take all reasonable steps to prevent the loss or compromise of classified material whether accidentally or from deliberate or opportunist attack.

10. Once the Contract has been awarded, where the Defence Supplier is required to store or process UK MOD classified information electronically, they shall comply with the requirements specified in ISNs, Defence Condition 658 and Defence Standard 05-138. Details can be found at the links below:

<https://www.gov.uk/government/publications/industry-security-notice-isns>.

<https://www.dstan.mod.uk/toolset/05/138/000003000.pdf>

<https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down>

11. All UK classified material including documents, media and other assets shall be physically secured to prevent unauthorised access. When not in use UK classified material shall be handled with care to prevent loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE material shall be stored under lock and key and shall be placed in a lockable room, cabinets, drawers or safe and the keys/combinations shall be controlled.

12. Disclosure of UK classified material shall be strictly controlled in accordance with the "need to know" principle. Except with the written consent of the Authority, the Defence Supplier shall not disclose the Contract or any provision thereof to any person other than to a person directly employed by the Defence Supplier or Subcontractor.

13. Except with the consent in writing of the Authority the Defence Supplier shall not make use of the Contract or any classified material issued or provided by or on behalf of the Authority otherwise than for the purpose of the Contract, and, same as provided for in paragraph 9 above, the Defence Supplier shall not make use of any article or part thereof similar to the articles for any other purpose.

14. Subject to any intellectual property rights of third parties, nothing in this Security Condition shall restrict the Defence Supplier from using any specifications, plans, drawings and other documents generated outside of this Contract.

15. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and shall be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 37.

### **Access**

16. Access to UK classified material shall be confined to those individuals who have a "need-to-know", have been made aware of the requirement to protect the material and whose access is essential for the purpose of their duties.

17. The Defence Supplier shall ensure that all individuals requiring access to UK OFFICIAL and UK OFFICIAL-SENSITIVE material have undergone basic recruitment checks. This

should include establishing proof of identity; confirming that they satisfy all legal requirements for employment by the Defence Supplier; and verification of their employment record. Criminal record checks should also be undertaken where permissible under national/local laws and regulations. This is in keeping with the core principles set out in the UK Government (HMG) Baseline Personnel Security Standard (BPSS) which can be found at:

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/714002/HMG\\_Baseline\\_Personnel\\_Security\\_Standard\\_-\\_May\\_2018.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf)

### **Hard Copy Distribution**

18. UK OFFICIAL and UK OFFICIAL-SENSITIVE documents may be distributed internally and externally of Defence Supplier premises. To maintain confidentiality, integrity and availability, distribution shall be controlled such that access to documents is only by authorised personnel. They may be sent by ordinary post in a single envelope. The words UK OFFICIAL or UK OFFICIAL-SENSITIVE must not appear on the envelope. The envelope must bear a stamp or marking that clearly indicates the full address of the office from which it was sent. Commercial Couriers may be used.

19. Advice on the distribution of UK OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of UK OFFICIAL-SENSITIVE shall be sought from the Authority.

### **Electronic Communication and Telephony and Facsimile Services**

20. UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a National Cyber Security Centre (NCSC) Commercial Product Assurance (CPA) cryptographic product or a UK MOD approved cryptographic technique such as Transmission Layer Security (TLS). In the case of TLS both the sender and recipient organisations must have TLS enabled. Details of the required TLS implementation and CPA scheme are available at:

<https://www.ncsc.gov.uk/guidance/tls-external-facing-services>  
<https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa>

21. Exceptionally, in urgent cases UK OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so, but only with the prior approval of the Authority. However, it shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the Authority require. Such limitations including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the information.

22. UK OFFICIAL and UK OFFICIAL-SENSITIVE information may be discussed verbally on corporate telephones and other corporate electronic devices with persons located both within the country of the Defence Supplier and overseas. UK OFFICIAL-SENSITIVE information should only be discussed where there is a strong business need to do so.

23. UK OFFICIAL information may be faxed to recipients located both within the country of the Defence Supplier and overseas, however UK OFFICIAL-SENSITIVE information may

be transmitted only where there is a strong business case to do so and only with the prior approval of the Authority.

### **Use of Information Systems**

24. The detailed functions that must be provided by an IT system to satisfy the minimum requirements cannot all be described here in specific detail; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

25. The Defence Supplier should ensure **10 Steps to Cyber Security** (Link below) is applied in a proportionate manner for each IT and communications system storing, processing or generating UK OFFICIAL or UK OFFICIAL-SENSITIVE information.

<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>

26. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum security requirements for processing and accessing UK OFFICIAL and UK OFFICIAL-SENSITIVE information on IT systems.

a. Access. Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of “*least privilege*” will be applied to System Administrators. Users of the IT System (Administrators) should not conduct ‘standard’ User functions using their privileged accounts.

b. Identification and Authentication (ID&A). All systems are to have the following functionality:

(1) Up-to-date lists of authorised users.

(2) Positive identification of all users at the start of each processing session

c. Passwords. Passwords are part of most ID&A security measures. Passwords are to be “strong” using an appropriate method to achieve this, e.g., including numeric and “special” characters (if permitted by the system) as well as alphabetic characters.

d. Internal Access Control. All systems are to have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission. Unless the Authority authorises otherwise, UK OFFICIAL-SENSITIVE information may only be transmitted or accessed electronically (e.g., point to point computer links) via a public network like the Internet, using a CPA product or equivalent as described in paragraph 20 above.

f. Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.

(1) The following events shall always be recorded:

(a) All log on attempts whether successful or failed,

(b) Log off (including time out where applicable),

(c) The creation, deletion or alteration of access rights and privileges,

(d) The creation, deletion or alteration of passwords.

(2) For each of the events listed above, the following information is to be recorded:

- (a) Type of event,
- (b) User ID,
- (c) Date & Time,
- (d) Device ID.

(3) The accounting records are to have a facility to provide the System Manager with a hard copy of all or selected activity. There also must be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know. If the operating system is unable to provide this, then the equipment must be protected by physical means when not in use i.e., locked away or the hard drive removed and locked away.

g. Integrity & Availability. The following supporting measures are to be implemented:

- (1) Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g., viruses and power supply variations),
- (2) Defined Business Contingency Plan,
- (3) Data backup with local storage,
- (4) Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software),
- (5) Operating systems, applications and firmware should be supported,
- (6) Patching of Operating Systems and Applications used are to be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.

h. Logon Banners. Wherever possible, a "Logon Banner" will be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring. A suggested format for the text (depending on national legal requirements) could be: *"Unauthorised access to this computer system may constitute a criminal offence"*.

i. Unattended Terminals. Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

j. Internet Connections. Computer systems must not be connected direct to the Internet or "un-trusted" systems unless protected by a firewall (a software based personal firewall is the minimum, but risk assessment and management must be used to identify whether this is sufficient).

k. Disposal. Before IT storage media (e.g., disks) are disposed of, an erasure product must be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

## **Portable Electronic Devices**

27. Portable Electronic Devices holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 20 above.

28. Unencrypted Portable Electronic Device and drives containing personal data are not to be taken outside of secure sites<sup>4</sup>. For the avoidance of doubt the term “drives” includes all removable, recordable media e.g., memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.

29. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

30. Portable Electronic Devices holding the Authorities’ data are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the Portable Electronic Device is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

## **Loss and Incident Reporting**

31. The Defence Supplier shall immediately report any loss or otherwise compromise of any Defence Related Classified Material to the Authority. The term Defence Related Classified Material includes any information or asset that has been given a security classification by the UK MOD. The term also includes classified information and assets held by UK Defence Suppliers which are owned by a third party e.g., NATO or another country for which the UK MOD is responsible.

32. In addition, any loss or otherwise compromise of Defence Related Classified Material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP). This will assist the UK MOD in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD’s Chief Information Officer (CIO) and, as appropriate, the Defence Supplier concerned. The UK MOD Defence Industry WARP will also advise the Defence Supplier what further action is required to be undertaken.

### **UK MOD Defence Industry WARP Contact Details**

**Email:** [DefenceWARP@mod.gov.uk](mailto:DefenceWARP@mod.gov.uk) (OFFICIAL with no NTK restrictions)

**RLI Email:** [defencewarp@modnet.r.mil.uk](mailto:defencewarp@modnet.r.mil.uk) (MULTIUSER)

**Telephone (Office hours):** +44 (0) 3001 583 640

**Mail:** Defence Industry WARP, DE&S PSyA Office

MOD Abbey Wood, NH2 Poplar-1 #2004, Bristol, BS34 8JH

33. Reporting instructions for any security incidents involving Defence Related Classified Material can be found in the Incident Reporting Industry Security Notice at:

<https://www.gov.uk/government/publications/industry-security-notices-isns>

## **Subcontracts**

---

<sup>4</sup> Secure Sites are defined as either Government premises or a secured office on the Defence Supplier premises.

34. Where the Defence Supplier wishes to subcontract any elements of a Contract to Subcontractors within its own country or to Subcontractors located in the UK such subcontracts will be notified to the Authority. The Defence Supplier shall ensure that these Security Conditions are incorporated within the subcontract document.

35. The prior approval of the Authority shall be obtained should the Defence Supplier wish to subcontract any UK OFFICIAL-SENSITIVE elements of the Contract to a Subcontractor facility located in another (third party) country. The first page of MOD Form 1686 (F1686) is to be used for seeking such approval. The MOD Form 1686 can be found in the "Subcontracting or Collaborating on Classified MOD Programmes ISN" at the link below:

<https://www.gov.uk/government/publications/industry-security-notices-isns>

36. If the subcontract is approved, the Defence Supplier shall flow down the Security Conditions in line with paragraph 34 above to the Subcontractor. Defence Suppliers located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

### **Physical Destruction**

37. As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when the classified material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Defence Supplier to be necessary or desirable. Unwanted UK OFFICIAL-SENSITIVE classified material which cannot be destroyed in such a way shall be returned to the Authority.

### **Private Venture Activities**

38. Private Venture (PV) funded (i.e., non-MOD funded) defence related projects and technology fall within one of the following three categories:

- a. Variants. Variants of standard defence equipment under research, development or in production, e.g., aircraft, military vehicles or ships, etc. with non-standard equipment or fitments, offered to meet special customer requirements or to avoid security or commercial difficulties associated with the sale of an item in-Service with UK Armed Forces.
- b. Derivatives. Equipment for military or civil use that is not based on standard Service designs but is dependent upon expertise or technology acquired in the course of defence contracts.
- c. Freelance. Equipment of defence importance that is in no way based on information gained from defence contracts.

39. UK Defence Suppliers shall ensure that any PV activity that falls into one of the above categories has been formally security graded by the MOD Directorate of Security and Resilience. Please see PV guidance on the following website further information:

<https://www.gov.uk/government/publications/private-venture-pv-grading-and-exhibition-clearance-information-sheets>

### **Publicity Material**



40. Defence Suppliers wishing to release any publicity material or display assets that arises from a Contract to which these Security Conditions apply must seek the prior approval of the Authority. Publicity material includes open publication in the Defence Supplier's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the UK Government.

41. For UK Defence Suppliers where the exhibition assets relate to multiple Delivery Teams or for Private Venture defence related classified material where there is no defined Delivery Team, the Defence Supplier shall request clearance for exhibition from the Directorate of Security and Resilience. See the MOD Exhibition Guidance on the following website for further information:

<https://www.gov.uk/government/publications/private-venture-pv-grading-and-exhibition-clearance-information-sheets>

### **Export sales/promotion**

42. The MOD Form 680 (F680) security procedure enables MOD to control when, how, and if defence related classified material is released by UK Defence Suppliers to foreign entities for the purposes of promotion or sales of equipment or services. Before undertaking any targeted promotion or demonstration or entering into any contractual commitments involving the sale or release of defence equipment, information or technology classified UK OFFICIAL-SENSITIVE or above to a foreign entity, a UK Defence Supplier shall obtain F680 approval from the Export Control Joint Unit (ECJU) MOD Team. This includes assets classified UK OFFICIAL-SENSITIVE or above either developed to meet a UK MOD requirement or Private Venture (PV) equipment, as formally advised in a Security Aspects Letter (SAL) issued by the relevant Authority, or PV Security Grading issued by the MOD Directorate of Security and Resilience. Guidance regarding the F680 procedure issued by ECJU can be found at:

<https://www.gov.uk/government/publications/ministry-of-defence-form-680-procedure-guidance>

43. If a Defence Supplier has received an approval to subcontract, under an MOD Form 1686 (F1686), for development/production of parts of an equipment, that approval also permits the production of additional quantities for supply to an export customer, when the Defence Supplier has MOD Form 680 approval for supply of the complete equipment, as long as:

- a. they are identical, except for component obsolescence, to items produced under the UK programme that the approval to subcontract relates to; and
- b. no additional OFFICIAL-SENSITIVE or above material is required to be released to the overseas Subcontractor.

### **Interpretation/Guidance**

44. Advice regarding the interpretation of the above requirements should be sought from the Authority.

45. Further requirements, advice and guidance for the protection of UK classified material at the level of UK OFFICIAL and UK OFFICIAL-SENSITIVE may be found in Industry Security Notices at:

<https://www.gov.uk/government/publications/industry-security-notices-isns>

### **Audit**

Where considered necessary by the Authority the Defence Supplier shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Defence Supplier's processes and facilities by representatives of the Defence Supplier's National/Designated Security Authorities or the Authority to ensure compliance with these requirements



**Annex D to SAL Apprentice Training Contract****Dated: 17/10/2024****OFFICIAL SECRETS ACT SECTION 2****Defence**

1. A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of any information, document or other article relating to defence which is or has been in his possession by virtue of his position as such.
2. For the purposes of subsection 1. above, a disclosure is damaging if:
  - (a) It damages the capability of, or of any part of, the armed forces of the Crown to carry out their tasks or leads to loss of life or injury to members of those forces or serious damage to the equipment or installations of those forces; or
  - (b) Otherwise than as mentioned in paragraph a. above, it endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests or endangers the safety of British citizens abroad; or
  - (c) It is of information or of a document or article which is such that its unauthorised disclosure would be likely to have any of those effects.
- (d)
3. It is a defense for a person charged with an offence under this section to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question related to Defence or that its disclosure would be damaging within the meaning of subsection 1. above.
- (e)
4. In this section 'Defence' means:
  - (f)
  - a. The size, shape, organization, logistics, order of battle, deployment, operations, state of readiness and training of the armed forces of the Crown;
  - b. The weapons, stores or other equipment of those forces and the invention, development, production and operation of such equipment and research relating to it;
  - (g)
  - c. Defence policy and strategy and military planning and intelligence;
  - (h)
  - d. Plans and measures for the maintenance of essential supplies and services that are or would be needed in time of war.
  - (i)

***Contractor's Personnel*****DEFCON 76*****At Government Establishments***

Edition 11/22

---

**Definitions**

1. Reference in this Condition to:
  - a) 'Government Establishment' or 'site' shall be deemed to include any of His Majesty's Ships or Vessels and Service Stations;
  - b) 'Officer in Charge' shall be deemed to include Officers Commanding Service Stations, Ships' Masters or Senior Officers, and Heads of Government Establishments; and
  - c) 'Contractor's Representative(s)' shall be deemed to include the Contractor's employees, agents and subcontractors.

**General**

2. The following general provisions apply:
  - a) The Officer in Charge shall provide such available administrative and technical facilities for the Contractor's Representatives employed at Government Establishments for the purpose of the Contract as may be necessary for the effective and economical discharge of work under the Contract. These facilities will be provided free of charge unless otherwise stated in the Contract. The status to be accorded to the Contractor's Representatives for messing purposes will be at the discretion of the Officer in Charge.
  - b) Any land or premises (including temporary buildings) made available to the Contractor by the Authority in connection with the Contract shall be made available to the Contractor free of charge, unless otherwise stated in the Contract, and shall be used by the Contractor solely for the purposes of performing the Contract. The Contractor shall have the use of such land or premises as licensee and shall vacate the same upon completion of the Contract. Any utilities required by the Contractor shall be subject to the charges set out in the Contract.
  - c) The Contractor shall have no claim against the Authority for any additional cost or delay occasioned by the closure for holidays of Government Establishments, where this is made known to them prior to entering into the Contract.

**Liability In Respect Of Damage To Government Property**

3. Without prejudice to the provisions of DEFCON 611 (Issued Property) and of DEFCON 612 (Loss of or Damage to the Articles), where those conditions form part of the Contract, the Contractor shall, except as otherwise provided for in the Contract, make good or, at the option of the Authority, pay compensation for all damage occurring to any Government Property, which includes land or buildings, occasioned by the Contractor, or by any of their Representatives, arising from the Contractor's or their Representatives' presence on a Government Establishment

in connection with the Contract, provided that this Condition shall not apply to the extent that the Contractor is able to show that any such damage was not caused or contributed to by any circumstances within the Contractor's or their Representatives' reasonable control.

4. The total liability of the Contractor under Clause 3 herein shall be subject to any limitation specified in the Contract.

## **Contractor's Property**

5. All property of the Contractor and their Representatives shall be at the risk of the Contractor whilst it is on any Government Establishment, and the Authority shall accept no liability for any loss or damage howsoever occurring thereto or caused thereby, except as follows:

- a) where any such loss or damage was caused or contributed to by any act, neglect or default of any Government Servant, agent or contractor then the Authority shall accept liability therefor to the extent to which such loss or damage is so caused or contributed to as aforesaid; and
- b) where any property of the Contractor has been taken on charge by the Officer in Charge, and a proper receipt has been given therefor, then the Authority shall be liable for any loss or damage occurring to that property while held on such charge as aforesaid.

## **Contractor's Representatives**

6. The Contractor shall submit in writing to the Authority for approval, initially and as necessary from time to time, a list of their Representatives who may need to enter a Government Establishment for the purpose of, or in connection with, work under the Contract, giving such particulars as the Authority may require, including full details of birthplace and parentage of any such Representative who:

- a) was not born in the United Kingdom; or
- b) if they were born in the United Kingdom, were born of parents either or both of whom were not born in the United Kingdom.

7. The Authority shall issue passes for those Representatives who are approved by it in accordance with Clause 6 herein for admission to a Government Establishment and a Representative shall not be admitted unless in possession of such a pass. Passes shall remain the property of the Authority and shall be surrendered on demand or on completion of the work.

8. Notwithstanding the provisions of Clauses 6 and 7 hereof if, in the opinion of the Authority, any Representative of the Contractor shall misconduct themselves, or it shall not be in the public interest for any person to be employed or engaged by the Contractor, the Contractor shall remove such person without delay on being required to do so and shall cause the work to be performed by such other person as may be necessary.

9. The decision of the Authority upon any matter arising under Clauses 6 to 8 inclusive shall be final and conclusive.

## **Observance Of Regulations**

10. The following provisions apply:

- a) The Contractor shall ensure that their Representatives have the necessary probity (by undertaking the

Government's Baseline Personnel Security Standard) and, where applicable, are cleared to the appropriate level of security<sup>5</sup> when employed within the boundaries of a Government Establishment.

- b) Where the Contractor requires information on the Government's Baseline Personnel Security Standard (the Standard) or security clearance for their Representatives or is not in possession of the relevant rules, regulations or requires guidance on them, they shall apply in the first instance to the Project Manager/Equipment Support Manager.
- c) On request, the Contractor shall be able to demonstrate to the Authority that the Contractor's processes to assure compliance with the standard have been carried out satisfactorily. Where that assurance is not already in place, the Contractor shall permit the Authority to inspect the processes being applied by the Contractor to comply with the Standard.
- d) The Contractor shall comply and shall ensure that their Representatives comply with the rules, regulations and requirements that are in force whilst at that Establishment which shall be provided by the Authority on request.
- e) When on board ship, compliance with the rules, regulations, and requirements shall be in accordance with the Ship's Regulations as interpreted by the Officer in Charge. Details of those rules, regulations and requirements shall be provided on request by the Officer in Charge.

## Transport Overseas

11. Where the Contractor's Representatives are required by the Contract to join or visit a Government Establishment overseas, transport between the United Kingdom and the place of duty (but excluding transport within the United Kingdom) shall be provided free of charge by the Authority whenever possible, normally by Royal Air Force or by MOD chartered aircraft. The Contractor shall make such arrangements through the Project Manager/Equipment Support Manager named for this purpose in the Contract. When such transport is not available within a reasonable time, or in circumstances where the Contractor wishes their Representatives to accompany materiel for installation which they are to arrange to be delivered, the Contractor shall make their own transport arrangements. The Authority shall reimburse the Contractor's costs for such transport of their Representatives on presentation of evidence supporting the use of alternative transport and of the costs involved. Transport of the Contractor's Representatives locally overseas which is necessary for the purposes of the Contract shall be provided wherever possible by the Authority and, where so provided, will be free of charge.

## Medical Treatment Overseas

12. Out-patient medical treatment given to the Contractor's Representatives by a Service Medical Officer or other Government Medical Officer at a Government Establishment overseas shall be free of charge. Treatment in a Service hospital or medical centre, dental treatment, the provision of dentures or spectacles, conveyance to and from a hospital, medical centre or surgery not within the Establishment, and transportation of the Contractor's Representatives back to the United Kingdom, or elsewhere, for medical reasons, shall be charged to the Contractor at the appropriate local rate.

---

<sup>5</sup> DM criteria not provided for contract publishing. Further details from the Authority

## Injuries, Disease And Dangerous Occurrences

13. The Contractor shall report any injury, disease or dangerous occurrence at any Government Establishment arising out of the performance of this Contract, which is required to be reported under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) to the Officer in Charge of the relevant Government Establishment. This would be in addition to any report, which the Contractor may be required to submit under RIDDOR to the relevant enforcing authority (e.g. Health and Safety Executive or Local Authority).

## Dependants Of Contractor's Representatives

14. No assistance from public funds, and no messing facilities, accommodation or transport overseas shall be provided for dependants or members of the families of the Contractor's Representatives. Medical or necessary dental treatment may, however, be provided for dependants or members of families on repayment at current MOD rates. **Provision Of Funds Overseas**

15. The Contractor shall, wherever possible, arrange for funds to be provided to their Representatives overseas through normal banking channels (e.g. by travellers cheques). If banking or other suitable facilities are not available, the Authority shall, upon request by the Contractor and subject to any reasonable limitation required by the Contractor, make arrangements for payments, converted at the prevailing rate of exchange (where applicable), to be made by the Establishment to which the Contractor's Representatives are attached. All such advances made by the Authority shall be recovered from the Contractor.

## Health And Safety Hazard Control

16. Where the Contractor enters a Government Establishment for the purpose of performing work under the Contract:

- a) The Contractor shall notify the Officer in Charge or the site project liaison officer or overseeing officer nominated in the Contract of:
  - i. any health and safety hazards associated with the work to be performed by them or any of their Representatives; ii. any foreseeable risks to the health and safety of all persons associated with such hazards; and iii. any precautions to be taken by them as well as any precautions which, in their opinion, ought to be taken by the Authority, in order to control such risks.
- b) The Authority shall notify the Contractor of:
  - i. any health and safety hazards which may be encountered by the Contractor or any of their Representatives on the Government Establishment; ii. any foreseeable risks to the health and safety of the Contractor or any of their Representatives, associated with such hazards; and iii. any precautions to be taken by the Authority as well as any precautions which, in its opinion, ought to be taken by the Contractor, in order to control such risks.
- c) The Contractor shall notify their Representatives of and, where appropriate, provide adequate instruction in relation to:
  - i. the hazards, risks and precautions notified by them to the Authority under sub-Clause 16.a); ii. the hazards, risks and precautions notified by the Authority to the Contractor under sub-Clause 16.b); and iii. the precautions which, in their opinion, ought to be taken by their Representatives in order to control those risks.

- d) The Contractor shall provide the Officer in Charge or the site project liaison officer or overseeing officer nominated in the Contract with:
  - i. copies of those sections of their own and, where appropriate, their Representatives' Safety Policies which are relevant to the risks notified under sub- Clause 16.a);
  - ii. copies of any related risk assessments; and iii. copies of any notifications and instructions issued by them to their Representatives under sub- Clause 16.c).
- e) The Authority shall provide the Contractor with:
  - i. copies of those sections of its own Safety Policies which are relevant to the risks notified under sub-Clause 16.b); ii. copies of any related risk assessments; and iii. copies of any notifications and instructions issued by it to its employees similar to those called for from the Contractor under sub-Clause 16.c).

## DEFCON 531: DISCLOSURE OF INFORMATION<sup>7</sup>

1. 'Information' means any information in any written or other tangible form disclosed to one party by or on behalf of the other party under or in connection with the Contract, including information provided in the tender or negotiations which preceded the award of the Contract.
2. Subject to Clauses 5 to 10 each party:
  - a. shall treat in confidence all Information it receives from the other;
  - b. shall not disclose any of that Information to any third party without the prior written consent of the other party, which consent shall not unreasonably be withheld, except that the Contractor may disclose Information in confidence, without prior consent, to such persons and to such extent as may be necessary for the performance of the Contract;
  - c. shall not use any of that Information otherwise than for the purpose of the Contract; and
  - d. shall not copy any of that Information except to the extent necessary for the purpose of exercising its rights of use and disclosure under the Contract.
3. The Contractor shall take all reasonable precautions necessary to ensure that all Information disclosed to the Contractor by or on behalf of the Authority under or in connection with the Contract:
  - a. is disclosed to their employees and sub-contractors, only to the extent necessary for the performance of the Contract; and
  - b. is treated in confidence by them and not disclosed except with prior written consent or used otherwise than for the purpose of performing work or having work performed for the Authority under the Contract or any subcontract under it.
4. The Contractor shall ensure that their employees are aware of their arrangements for discharging the obligations at Clauses 2 and 3 before they receive Information and take such steps as may be reasonably practical to enforce such arrangements.
5. A party shall not be in breach of Clauses, 3, 7, 8 and 9 to the extent that either party:
  - a. exercises rights of use or disclosure granted otherwise than in consequence of, or under, the Contract;
  - b. has the right to use or disclose the Information in accordance with other conditions of the Contract; or c) can show:
    - i. that the Information was or has become published or publicly available for use otherwise than in breach of any provision of the Contract or any other agreement between the parties;
    - ii. that the Information was already known to it (without restrictions on disclosure or use) prior to it receiving it under or in connection with the Contract;
    - iii. that the Information was received without restriction on further disclosure from a third party who lawfully acquired it and who is under no obligation restricting its disclosure; or iv. from its records that the same information was derived independently of that received under or in connection with the Contract; provided the relationship to any other Information is not revealed.
6. Neither party shall be in breach of this Condition where it can show that any disclosure of Information was made solely and to the extent necessary to comply with a statutory, judicial or parliamentary obligation. Where such a disclosure is made, the party making the disclosure shall ensure that the recipient of the Information is made aware of and asked to

respect its confidentiality. Such disclosure shall in no way diminish the obligations of the parties under this Condition.

7. The Authority may disclose the Information:
  - a. to any Central Government Body for any proper purpose of the Authority or of the relevant Central Government Body, which shall include disclosure to the Cabinet Office and / or HM Treasury for the purpose of ensuring effective cross-Government procurement processes, including value for money and related purposes. Where such a disclosure is made the Authority shall ensure that the recipient is made aware of its confidentiality;
  - b. to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;
  - c. subject to Clause 8 below, to the extent that the Authority (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;
  - d. subject to Clause 8 below, on a confidential basis to a professional adviser, consultant or other person engaged by any of the entities defined in DEFCON 501 (including benchmarking organisation) for any purpose relating to or connected with this Contract;
  - e. on a confidential basis for the purpose of the exercise of its rights under the Contract; or
  - f. on a confidential basis to a proposed body in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under the Contract; and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Authority under this DEFCON.
  
8. Where the Authority intends to disclose Information to a commercial entity which is not a Central Government Body in accordance with Clauses 7.c or 7.d above, the Authority will endeavour to provide the Contractor with 3 Business Days' notice in advance of such disclosure. In relation to a disclosure of Information made under Clause 7.c above, if reasonably requested by the Contractor within 2 Business Days of such notice being given, where the Authority has not already done so, it will endeavour to procure from the intended recipient of the Information an agreement containing confidentiality terms the same as, or substantially similar to, those placed on the Authority under this DEFCON.
  
9. Before sharing any Information in accordance with clause 7 above, the Authority may redact the Information. Any decision to redact information made by the Authority shall be final.
  
10. The Authority shall not be in breach of the Contract where it can show that any disclosure of Information is made solely and to the extent necessary to comply with the Freedom of Information Act 2000 ("the Act") or the Environmental Information Regulations 2004 ("the Regulations"). To the extent permitted by the time for compliance under the Act or the Regulations, the Authority shall consult the Contractor where the Authority is considering the disclosure of Information under the Act or the Regulations and, in any event, shall provide prior notification to the Contractor of any decision to disclose the Information. The Contractor acknowledges and accepts that its representations on disclosure during consultation may not be determinative and that the decision whether to disclose Information in order to comply with the Act or the Regulations is a matter in which the Authority shall exercise its own discretion, subject always to the provisions of the Act or the Regulations. For the avoidance of doubt, nothing in this Condition shall affect the Contractor's rights at law.
  
11. Nothing in this Condition shall affect the parties' obligations of confidentiality where information is disclosed orally in confidence.





# CYBER DEFCON 658

Edition 10/22

---

## 1. Definitions

1.1. In this Condition the following words and expressions shall have the meanings given to them, except where the context requires a different meaning:

**“Associated Company”** means:

- (a) any associated company of the Contractor from time to time within the meaning of Section 449 of the Corporate Tax Act 2010 or any subordinate legislation; and
- (b) any parent undertaking or subsidiary undertaking of the Contractor from time to time within the meaning of section 1162 Companies Act 2006 and it is further agreed that where the ownership of shares in any such undertaking have been pledged or transferred to a third party by way of security, the original parent shall still be considered a member of the subsidiary undertaking; **“Cyber Risk Profile”**

means the level of cyber risk relating to this Contract assessed by the Authority or in relation to any Sub-contract assessed by the Contractor, in each case in accordance with the Cyber Security Model;

**“Cyber Implementation Plan”** means the plan referred to in Clause 3 of this Condition;

**“Cyber Security Incident”** means an event, act or omission which gives rise or may give rise to:

- (j) unauthorised access to an information system or electronic communications network on which MOD Identifiable Information resides;
- (k) disruption or change of the operation (including but not limited to takeover of control) of an information system or electronic communications network on which MOD Identifiable Information resides;
- (l) unauthorised destruction, damage, deletion or the change of MOD Identifiable Information residing in an information system or electronic communications network;
- (m) unauthorised or unintentional removal or limiting the possibility to use MOD Identifiable Information residing in an information system or electronic communications network; or
- (n) the appropriation, publication, dissemination or any other use of non-public MOD Identifiable Information by persons unauthorised to do so;

**“Cyber Security Instructions”** means DEFSTAN 05-138, together with any relevant ISN and specific security instructions relating to this Contract issued by the Authority to the Contractor;

**“Cyber Security Model”** and **“CSM”** mean the process by which the Authority ensures that MOD Identifiable Information is adequately protected from Cyber Security Incident and includes the CSM Risk Assessment Process, DEFSTAN 05-138 and the CSM Supplier Assurance Questionnaire conducted via the Supplier Cyber Protection Service; **“CSM Risk Assessment Process”** means the

risk assessment process which forms part of the Cyber Security Model and is used to measure the Cyber Risk Profile for this Contract and any Sub-contract; **“CSM Supplier Assurance Questionnaire”** means the supplier assessment questionnaire which forms part of the Cyber Security Model and is to be used by the Contractor to demonstrate compliance with this Condition;

**“Data”** means any 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; **“DEFSTAN 05-138”** means the Defence Standard 05-138 as amended or replaced from time to time;

**“Electronic Information”** means all information generated, processed, transferred or otherwise dealt with under or in connection with the Contract, including but not limited to Data, recorded or preserved in electronic form and held on any information system or electronic communications network;

**“Good Industry Practice”** means in relation to any undertaking and any circumstances, the exercise of skill, diligence, prudence, foresight and judgment and the making of any expenditure that would reasonably be expected from a skilled person in the same type of undertaking under the same or similar circumstances;

**“ISN”** means Industry Security Notices issued by the Authority to the Contractor whether directly or by issue on the gov.uk website at:

<https://www.gov.uk/government/publications/industry-security-noticesisns>;

**“JSyCC WARP”** means the Joint Security Co-ordination Centre MOD Defence Industry Warning, Advice and Reporting Point or any successor body notified by way of ISN;

**“MOD Identifiable Information”** means all Electronic Information which is attributed to or could identify an existing or proposed MOD capability, defence activities or personnel and which the MOD requires to be protected against loss, misuse, corruption, alteration and unauthorised disclosure;

**“NSA/DSA”** means, as appropriate, the National or Designated Security Authority of the Contractor that is responsible for the oversight of the security requirements to be applied by the Contractor and for ensuring compliance with applicable national security regulations;

**“Sites”** means any premises from which Contractor Deliverables are provided in connection with this Contract or from which the Contractor or any relevant Sub-contractor manages, organises or otherwise directs the provision or the use of the Contractor Deliverables and/or any sites from which the Contractor or any relevant Sub-contractor generates, processes, stores or transmits MOD Identifiable Information in relation to this Contract;

**“Sub-contract”** means any sub-contract awarded directly by the Contractor as a consequence of or in connection with this Contract; **“Sub-contractor”** means a sub-contractor or any Associated Company of the Contractor who provides Contractor Deliverables in connection with this Contract but only to the extent that the Sub-contractor processes, stores or transmits MOD Identifiable Information under their Subcontract;

**“Supplier Cyber Protection Service”** means the tool incorporating the CSM Risk Assessment Process and CSM Supplier Assurance Questionnaire.

## 2. **Authority Obligations** 2.1. The

Authority shall:

- 2.1.1. determine the Cyber Risk Profile appropriate to this Contract and notify the Contractor of the same at the earliest possible date; and
- 2.1.2. notify the Contractor as soon as reasonably practicable where the Authority reassesses the Cyber Risk Profile relating to this Contract, which shall be in accordance with Clause 7.

## 3. **Contractor Obligations**

3.1. The Contractor shall, and shall procure that their Sub-contractors shall:

- 3.1.1. comply with DEFSTAN 05-138 or, where applicable, the Cyber Implementation Plan attached to this Contract and for the avoidance of doubt any Cyber Implementation Plan shall be prepared and implemented in accordance with Good Industry Practice taking account of any risk-balance case and any mitigation measures required by the Authority and shall ensure that any measures taken to protect MOD Identifiable Information are no less stringent than those taken to protect their own proprietary information;
- 3.1.2. complete the CSM Risk Assessment Process in accordance with the Authority's instructions, ensuring that any change in the Cyber Risk Profile is notified to any affected Sub-contractor, and complete a further CSM Risk Assessment or CSM Supplier Assurance Questionnaire where a change is proposed to the Contractor's supply chain or on receipt of any reasonable request by the Authority;
- 3.1.3. re-perform the CSM Supplier Assurance Questionnaire no less than once in each year of this Contract commencing on the first anniversary of completion of the CSM Supplier Assurance Questionnaire to demonstrate continued compliance with the Cyber Security Instructions;
- 3.1.4. having regard to the state of technological development, implement and maintain all appropriate technical and organisational security measures to discharge their obligations under this Condition in accordance with Good Industry Practice *provided always that* where there is a conflict between the Contractor's obligations under 3.1.1 above and this 3.1.4 the Contractor shall notify the Authority in accordance with the notification provisions in DEFSTAN 05-138 as soon as they become aware of the conflict and the Authority shall determine which standard or measure shall take precedence;
- 3.1.5. comply with all Cyber Security Instructions notified to it by the Authority as soon as reasonably practicable;
- 3.1.6. notify the JSyCC WARP in accordance with ISN 2017/03 as amended or updated from time to time and the Contractors NSA/DSA, and in the case of a Sub-contractor also notify the Contractor, immediately in writing as soon as they know or believe that a Cyber Security Incident has or may have taken place providing initial details of the circumstances of the incident and any mitigation measures already taken or intended to be taken, and providing further information in phases, as full details become available;
- 3.1.7. in coordination with their NSA/DSA, investigate any Cyber Security Incidents fully and promptly and co-operate with the Authority and its agents and representatives to take all steps to mitigate the impact of the Cyber Security Incident and minimise the likelihood of any further similar Cyber Security Incidents. For the avoidance of doubt, this shall include complying with any reasonable technical or organisational security measures deemed appropriate by the Authority and the Contractors NSA/DSA in the circumstances and taking into account the Cyber Risk Profile; and
- 3.1.8. consent to the Authority recording and using information obtained via the Supplier Cyber Protection Service in relation to the Contract for the purposes of the Cyber Security Model which shall include any agreed Cyber Implementation Plan. For the avoidance of doubt such information shall include the cyber security accreditation of the Contractor and/or Sub-contractor as appropriate; and
- 3.1.9. include provisions equivalent to those set out in the Annex to this Condition (the "equivalent provisions") in all relevant Subcontracts.

## 4. Management Of Sub-Contractors

- 4.1. Provided that it is reasonable in all the circumstances to do so, the Authority agrees that the Contractor shall be entitled to rely on the selfcertification by the Sub-contractor of their compliance with this Condition in accordance with 3.1.1 above.

- 4.2. Where a Sub-contractor notifies the Contractor that it cannot comply with the requirements of DEFSTAN 05-138, the Contractor shall require a Subcontractor to prepare and implement a Cyber Implementation Plan in accordance with Good Industry Practice taking account of any risk-balance case and any mitigation measures required by the Contractor and shall ensure that any measures taken to protect MOD Identifiable Information are no less stringent than those taken to protect the proprietary information of the Sub-contractor. Where the Contractor has reasonably relied on the Sub-contractor's self-certification and the Sub-contractor is subsequently found to be in breach of their obligations, the Contractor shall not be in breach of this Condition.
- 4.3. The Contractor shall, and shall require their Sub-contractors to, include provisions equivalent to those set out in the Annex to this Condition in all relevant Sub-contracts and shall notify the Authority in the event that they become aware of any material breach of the provisions set out in the Annex by their Sub-contractor.

## 5. Records

- 5.1. The Contractor shall keep and maintain, and shall ensure that any Subcontractor shall keep and maintain, until 6 years after termination or end of Contract term or final payment under this Contract, or as long a period as may be agreed between the Parties, full and accurate records including but not limited to:
- 5.1.1. copies of all documents required to demonstrate compliance with DEFSTAN 05-138 and this Condition, including but not limited to any information used to inform the CSM Risk Assessment Process and to carry out the CSM Supplier Assurance Questionnaire, together with any certificates issued to the Contractor and/or Sub-contractor; and
  - 5.1.2. copies of all documents demonstrating compliance with 3.1.5 and in relation to any notifications made under 3.1.6 and/or investigation under 3.1.7.
- 5.2. The Contractor shall, and shall ensure that any Sub-contractor shall, on request provide the Authority, the Authority's representatives and/or the Contractors NSA/DSA such access to those records under 5.1 as may be required in connection with this Contract.

## 6. Audit

- 6.1. In the event of a Cyber Security Incident the Contractor agrees that the Authority and its representatives, in coordination with the Contractor's NSA/DSA, may conduct such audits as are required to establish (i) the cause of the Cyber Security Incident, (ii) the impact of the Cyber Security Incident, (iii) the MOD Identifiable Information affected, and (iv) the work carried out by the Contractor to resolve the Cyber Security Incident and to mitigate the effects, to ensure that the Cyber Security Incident is resolved to the satisfaction of the Authority and the NSA/DSA.
- 6.2. In addition to the rights in 6.1 above the Authority or its representatives and/or the Contractor's NSA/DSA, either solely or in any combination, may at any time during the Contract and for a period of six (6) years after termination of the Contract or the end of the Contract term or final payment under the Contract whichever is the later, but not more than once in any calendar year, conduct an audit for the following purposes where the Contractor continues to hold MOD Identifiable Information:
- 6.2.1. to review and verify the integrity, confidentiality and security of any MOD Identifiable Information; and
  - 6.2.2. to review the Contractor's and/or any Sub-contractor's compliance with their obligations under DEFSTAN 05-138 or a Cyber Implementation Plan; and
  - 6.2.3. to review any records created during the provision of the Contractor Deliverables, including but not limited to any documents, reports and minutes which refer or relate to the Contractor Deliverables for the purposes of 5.1.1 and 5.1.2 above.
- 6.3. The Authority, acting reasonably and having regard to the confidentiality and security obligations owed by the Contractor to third parties, shall propose the scope of each audit in writing with a view to seeking the agreement of the Contractor but shall make the ultimate decision on the scope. For the avoidance of doubt the scope of the audit shall not grant the

Authority any unsupervised access to any of the Contractor's information systems or electronic communications networks. The Authority shall use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Contractor and/or Sub-contractor or delay the provision of the Contractor Deliverables and supplier information received by the Authority in connection with the audit shall be treated as confidential information.

- 6.4. The Contractor shall, and shall ensure that any Sub-contractor shall on demand provide the Authority and any relevant regulatory body, including the Contractor's NSA/DSA, (and/or their agents or representatives), together "the Auditors", with all reasonable co-operation and assistance in relation to each audit, including but not limited to:
  - 6.4.1. all information requested by the Authority within the permitted scope of the audit;
  - 6.4.2. reasonable access to any Sites controlled by the Contractor or any Associated Company used in the performance of the Contract to the extent required within the permitted scope of the audit and, where such Sites are outwith the control of the Contractor, shall secure sufficient rights of access for the Auditors as shall be necessary to allow audits to take place; and
  - 6.4.3. access to any relevant staff.
- 6.5. The Authority shall endeavour to (but is not obliged to) provide at least 15 calendar days' notice of its intention to conduct an audit.
- 6.6. The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under this Condition, unless the audit identifies a material breach of the terms of this Condition by the Contractor in which case the Contractor shall reimburse the Authority for all the Authority's reasonable costs incurred (which shall be evidence to the Contractor) in the course of the audit.
- 6.7. The Contractor shall in their Sub-contracts procure rights for the Authority to enforce the terms of clause 6 of this Condition in accordance with the Contracts (Rights of Third Parties) Act 1999.

## 7. General

- 7.1. On termination or expiry of this Contract the provisions of this Condition excepting 3.1.2 and 3.1.3 above shall continue in force so long as the Contractor and/or and Sub-contractor holds any MOD Identifiable Information relating to this Contract.
- 7.2. Termination or expiry of this Contract shall not affect any rights, remedies, obligations or liabilities of the Parties under this Condition that have accrued up to the date of termination or expiry, including but not limited to the right to claim damages in respect of any breach of the Contract which existed at or before the date of termination or expiry.
- 7.3. The Contractor agrees that the Authority has absolute discretion to determine changes to DEFSTAN 05-138 or the Cyber Risk Profile or both and issue new or updated Cyber Security Instructions. In the event that there is such a change to DEFSTAN 05-138 or the Cyber Risk Profile or both, then either Party may seek an adjustment to the Contract Price for any associated increase or decrease in costs and the Contractor may request an extension of time for compliance with such revised or amended DEFSTAN 05-138 or Cyber Risk Profile or both *provided always that* the Contractor shall seek to mitigate the impact on time and cost to the extent which it is reasonably practicable to do so and *further provided that* such costs shall not be allowed unless they are considered to be appropriate, attributable to the Contract and reasonable in all the circumstances.
- 7.4. Subject to 7.3 above, where the Contractor seeks such adjustment or extension, the Authority will proceed in accordance with DEFCON 620 or any agreed alternative change control procedure to determine the request for adjustment or extension. The Contractor must deliver a Contractor Change Proposal to the Authority within eight (8) weeks (or other period agreed by the parties) of the occurrence of the change in DEFSTAN 05138 or Cyber Risk Profile or both, identifying the impact of that change and accompanied by full details of the request for adjustment. For the avoidance of doubt, the Authority shall not be required to withdraw any Authority Notice of Change which may have been issued insofar as it relates to DEFSTAN 05-138 or the Cyber Risk Profile or both whether or not the Contractor

Change Proposal is rejected. If the Contractor does not agree with the Authority's determination, then the provisions of DEFCON 530 or any agreed alternative dispute resolution procedure provided for in the Contract shall apply.

- 7.5. The Contractor shall not recover any costs and/or other losses under or in connection with this Condition where such costs and/or other losses are recoverable or have been recovered by the Contractor elsewhere in this Contract or otherwise. For the avoidance of doubt this shall include but not be limited to the cost of implementing any upgrades or changes to any information system or electronic communications network whether in response to a Cyber Security Incident or otherwise, where the Contractor is able to or has recovered such sums in any other provision of this Contract or has recovered such costs and/or losses in other contracts between the Contractor and the Authority or with other bodies.

## **Annex to DEFCON 658**

### **Cyber**

### **Provisions to Be Included in Relevant Sub-Contracts**

#### **1. Definitions**

- 1.1. In this Condition the following words and expressions shall have the meanings given to them, except where the context requires a different meaning:

**“Associated Company”** means:

- (a) any associated company of the Sub-contractor from time to time within the meaning of Section 449 of the Corporate Tax Act 2010 or any subordinate legislation; and
- (b) any parent undertaking or subsidiary undertaking of the Subcontractor from time to time within the meaning of section 1162 Companies Act 2006 and it is further agreed that where the ownership of shares in any such undertaking have been pledged or transferred to a third party by way of security, the original parent shall still be considered a member of the subsidiary undertaking;

**“Cyber Risk Profile”** means the level of cyber risk relating to this Subcontract or any lower tier Sub-contract assessed in accordance with the Cyber Security Model;

**“Cyber Implementation Plan”** means the plan referred to in Clause 2 of this Condition;

**“Cyber Security Incident”** means an event, act or omission which gives rise or may give rise to:

- (a) unauthorised access to an information system or electronic communications network on which MOD Identifiable Information resides;
- (b) disruption or change of the operation (including but not limited to takeover of control) of an information system or electronic communications network on which MOD Identifiable Information resides;
- (c) unauthorised destruction, damage, deletion or the change of MOD Identifiable Information residing in an information system or electronic communications network;
- (d) unauthorised or unintentional removal or limiting the possibility to use MOD Identifiable Information residing in an information system or electronic communications network; or

- (e) the appropriation, publication, dissemination or any other use of non-public MOD Identifiable Information by persons unauthorised to do so.

**"Cyber Security Instructions"** means DEFSTAN 05-138, together with any relevant ISN and specific security instructions relating to this Subcontract issued by the MOD to the Prime Contractor;

**"Cyber Security Model"** and **"CSM"** mean the process by which the MOD ensures that MOD Identifiable Information is adequately protected from Cyber Security Incident and includes the CSM Risk Assessment Process, DEFSTAN 05-138 and the CSM Supplier Assurance Questionnaire conducted via the Supplier Cyber Protection Service;

**"CSM Risk Assessment Process"** means the risk assessment process which forms part of the Cyber Security Model and is used to measure the Cyber Risk Profile for this Sub-contract and any lower tier Sub-contract;

**"CSM Supplier Assurance Questionnaire"** means the supplier assessment questionnaire which forms part of the Cyber Security Model and is to be used by the Sub-contractor to demonstrate compliance with this Condition;

**"Data"** means any 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;

**"DEFSTAN 05-138"** means the Defence Standard 05-138 as amended or replaced from time to time;

**"Electronic Information"** means all information generated, processed, transferred or otherwise dealt with under or in connection with this Subcontract, including but not limited to Data, recorded or preserved in electronic form and held on any information system or electronic communications network;

**"Good Industry Practice"** means in relation to any undertaking and any circumstances, the exercise of skill, diligence, prudence, foresight and judgment and the making of any expenditure that would reasonably be expected from a skilled person in the same type of undertaking under the same or similar circumstances;

**"ISN"** means Industry Security Notices issued by the MOD to the Prime Contractor whether directly or by issue on the gov.uk website at:  
<https://www.gov.uk/government/publications/industry-security-noticesisns>;

**"JSyCC WARP"** means the Joint Security Co-ordination Centre MOD Defence Industry Warning, Advice and Reporting Point or any successor body notified by way of ISN;

**"MOD"** means the UK Ministry of Defence of 1 Horseguards, London acting by [ ] project team at [insert contact details];

**"MOD Identifiable Information"** means all Electronic Information which is attributed to or could identify an existing or proposed MOD capability, defence activities or personnel and which the MOD requires to be protected against loss, misuse, corruption, alteration and unauthorised disclosure;

**"Prime Contract"** means [contract reference] [insert details of prime contract] made between the MOD and the Contractor;

**"Prime Contractor"** means the Contractor named in the Prime Contract with MOD;



**“NSA/DSA”** means, as appropriate, the National or Designated Security Authority of the Prime or Sub-contractor that is responsible for the oversight of the security requirements to be applied by the Prime or Subcontractor and for ensuring compliance with applicable national security regulations;

**“Sites”** means any premises from which Contractor Deliverables are provided in connection with this Sub-contract or from which the Subcontractor or any relevant lower tier Sub-contractor manages, organises or otherwise directs the provision or the use of the Contractor Deliverables and/or any sites from which the Sub-contractor or any relevant lower tier Sub-contractor generates, processes, stores or transmits MOD Identifiable Information in relation to this Sub-contract;

**“Sub-contract”** means any sub-contract at any level of the supply chain, whether this Sub-contract which is awarded by the Prime Contractor or any related Sub-contract which is awarded by the Sub-Contractor or any lower tier Sub-contractor or Associated Company, which is entered into as a consequence of or in connection with this Sub-contract;

**“Sub-contractor”** means a sub-contractor of the Prime Contractor or any Associated Company whether a direct Sub-contractor or at any lower level of the supply chain who provides any Contractor Deliverables in connection with the Prime Contract but only to the extent that the Subcontractor processes, stores or transmits MOD Identifiable Information under their Sub-contract;

**“Supplier Cyber Protection Service”** means the tool incorporating the CSM Risk Assessment Process and CSM Supplier Assurance Questionnaire;

## 2. Sub-Contractor Obligations

2.1. The Sub-contractor shall, and shall procure that their lower tier Subcontractors shall:

- 2.1.1. comply with DEFSTAN 05-138 or, where applicable, the Cyber Implementation Plan attached to this Sub-contract and for the avoidance of doubt any Cyber Implementation Plan shall be prepared and implemented in accordance with Good Industry Practice taking account of any risk-balance case and any mitigation measures required by the MOD and the Prime Contractor and shall ensure that any measures taken to protect MOD Identifiable Information are no less stringent than those taken to protect their own proprietary information;
- 2.1.2. complete the CSM Risk Assessment Process in accordance with the MOD and the Prime Contractor's instructions, ensuring that any change in the Cyber Risk Profile is notified to the MOD, the Prime Contractor and any affected lower tier Sub-contractor, and complete a further CSM Risk Assessment or CSM Supplier Assurance Questionnaire where a change is proposed to the supply chain or on receipt of any reasonable request by the MOD;
- 2.1.3. re-perform the CSM Supplier Assurance Questionnaire no less than once in each year of this Sub-contract commencing on the first anniversary of completion of the CSM Supplier Assurance Questionnaire to demonstrate continued compliance with the Cyber Security Instructions;
- 2.1.4. having regard to the state of technological development, implement and maintain all appropriate technical and organisational security measures to discharge their obligations under this Condition in accordance with Good Industry Practice *provided always that* where there is a conflict between the Subcontractor's obligations under 2.1.1 above and this 2.1.4 the Sub-contractor shall notify the

Prime Contractor and the MOD in accordance with the notification provisions in DEFSTAN 05-138 as soon as they become aware of the conflict and the MOD shall determine which standard or measure shall take precedence;

- 2.1.5. comply with all Cyber Security Instructions notified to them by the MOD and/or the Prime Contractor as soon as reasonably practicable;
- 2.1.6. notify the JSyCC WARP in accordance with ISN 2017/03 as amended or updated from time to time and the Prime Contractor and the Sub-Contractor's NSA/DSA immediately in writing as soon as they know or believe that a Cyber Security Incident has or may have taken place providing initial details of the circumstances of the incident and any mitigation measures already taken or intended to be taken, and providing further information in phases, as full details become available;
- 2.1.7. in coordination with their NSA/DSA, investigate any Cyber Security Incidents fully and promptly and co-operate with the MOD, the Prime Contractor and their agents and representatives to take all steps to mitigate the impact of the Cyber Security Incident and minimise the likelihood of any further similar Cyber Security Incidents. For the avoidance of doubt, this shall include complying with any reasonable technical or organisational security measures deemed appropriate by the MOD and the relevant Prime and/or Sub-contractor's NSA/DSA in the circumstances and taking into account the Cyber Risk Profile; and
- 2.1.8. consent to the MOD recording and using information obtained via the Supplier Cyber Protection Service in relation to the Subcontract for the purposes of the Cyber Security Model which shall include any agreed Cyber Implementation Plan. For the avoidance of doubt such information shall include the cyber security accreditation of the Sub-contractor and/or lower tier Sub-contractor as appropriate; and
- 2.1.9. include provisions equivalent to this Condition in all lower tier Sub-contracts (the "equivalent provisions") and, where a lower tier Sub-contractor breaches terms implementing this Condition
  - in a Sub-contract, the Sub-contractor shall, and shall procure that their lower tier Sub-contractors shall, in exercising their rights or remedies under the relevant Sub-contract:
    - 2.1.9.1. notify the Prime Contractor and the MOD of any such breach and consult with the Prime Contractor and the MOD regarding any remedial or other measures which are proposed as a consequence of such breach, taking the MOD's views into consideration; and
    - 2.1.9.2. have regard to the equivalent provisions.

### 3. Records

- 3.1. The Sub-contractor shall keep and maintain, and shall ensure that any lower tier Sub-contractor shall keep and maintain, until six (6) years after termination of Contract term or final payment under this Sub-contract, or as long a period as may be agreed between the Parties, full and accurate records including but not limited to:
  - 3.1.1. copies of all documents required to demonstrate compliance with DEFSTAN 05-138 and this Condition, including but not limited to any information used to inform the CSM Risk Assessment Process and to carry out the CSM Supplier Assurance

Questionnaire, together with any certificates issued to the Sub-contractor and/or any lower tier Sub-contractor.

- 3.1.2. copies of all documents demonstrating compliance with 2.1.5 and in relation to any notifications made under 2.1.6 and/or investigation under 2.1.7.

3.2. The Sub-contractor shall, and shall ensure that any lower tier Subcontractor shall, on request provide the MOD, the MOD's representatives and/or the relevant Prime or Sub-contractor's NSA/DSA such access to those records under 3.1 as may be required in connection with this Subcontract.

## 4. Audit

4.1. In the event of a Cyber Security Incident the Sub-contractor agrees that the MOD and its representatives, in coordination with the relevant Prime or Sub-contractor's NSA/DSA, may conduct such audits as are required to establish (i) the cause of the Cyber Security Incident, (ii) the impact of the Cyber Security Incident, (iii) the MOD Identifiable Information affected, and (iv) the work carried out by the Sub-contractor to resolve the Cyber Security Incident and to mitigate the effects, to ensure that the Cyber Security Incident is resolved to the satisfaction of the MOD and the NSA/DSA.

4.2. In addition to the rights in 4.1 above, the Sub-contractor agrees that the MOD, its representatives and/or the relevant Prime or Sub-contractor's NSA/DSA, either solely or in any combination, may at any time during the Contract and for a period of six (6) years after termination of this Subcontract or the end of the Sub-contract term or final payment under the Sub-contract whichever is the later, but not more than once in any

calendar year, conduct an audit for the following purposes where the SubContractor continues to hold MOD Identifiable Information:

- 4.2.1. to review and verify the integrity, confidentiality and security of any MOD Identifiable Information;
- 4.2.2. to review the Sub-contractor's and/or any lower tier Subcontractor's compliance with their obligations under DEFSTAN 05-138 or a Cyber Implementation Plan; and
- 4.2.3. to review any records created during the provision of the Contractor Deliverables, including but not limited to any documents, reports and minutes which refer or relate to the Contractor Deliverables for the purposes of 3.1.1 and 3.1.2 above.

4.3. The MOD, acting reasonably and having regard to the confidentiality and security obligations owed by the Sub-contractor to third parties, shall propose the scope of each audit in writing with a view to seeking the agreement of the Sub-contractor but shall make the ultimate decision on the scope. For the avoidance of doubt the scope of the audit shall not grant the MOD any unsupervised access to any of the Sub-contractor's information systems or electronic communications networks. The MOD and the Prime Contractor shall use their reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Subcontractor and/or lower tier Sub-contractor or delay the provision of the Contractor Deliverables and supplier information received in connection with the audit shall be treated as confidential information.

4.4. The Sub-contractor shall, and shall ensure that any lower tier Subcontractor shall, on demand provide the MOD and any relevant regulatory body, including the relevant Prime or Sub-contractor's NSA/DSA, (and/or their agents or representatives), together "the Auditors", with

all reasonable co-operation and assistance in relation to each audit, including but not limited to:

- 4.4.1. all information requested by the MOD within the permitted scope of the audit;
- 4.4.2. reasonable access to any Sites controlled by the Sub-contractor or any Associated Company and any lower tier Sub-contractor used in the performance of the Sub-contract to the extent required within the permitted scope of the audit and, where such Sites are outwith the control of the Sub-contractor, shall secure sufficient rights of access for the Auditors as shall be necessary to allow audits to take place; and
- 4.4.3. access to any relevant staff.

- 4.5. Where the Prime Contractor is provided with notice of the audit by the MOD and/or the relevant NSA/DSA, the Prime Contractor shall endeavour to (but is not obliged to) provide at least 15 calendar days' notice to the Sub-contractor of the intention to conduct an audit.
- 4.6. The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under this Condition, unless the audit identifies a material breach of the terms of this Condition by the Sub-contractor and/or a lower tier Sub-contractor in which case the Sub-contractor shall reimburse the Prime Contractor and the MOD as appropriate for all the reasonable costs incurred in the course of the audit.
- 4.7. The Sub-Contractor shall in their lower tier Sub-contracts procure rights for the MOD to enforce the terms of this clause 4 of this Condition in accordance with the Contracts (Rights of Third Parties) Act 1999.

## 5. General

- 5.1. On termination or expiry of this Sub-contract the provisions of this Condition shall continue in force so long as the Sub-contractor and/or any lower tier Sub-contractor holds any MOD Identifiable Information relating to this Sub-contract.
- 5.2. Termination or expiry of this Sub-contract shall not affect any rights, remedies, obligations or liabilities of the Parties under this Condition that have accrued up to the date of termination or expiry, including but not limited to the right to claim damages in respect of any breach of this Subcontract which existed at or before the date of termination or expiry.
- 5.3. The Sub-contractor agrees that the MOD has absolute discretion to determine changes to DEFSTAN 05-138 or the Cyber Risk Profile or both and issue new or updated Cyber Security Instructions. In the event that there is such a change to DEFSTAN 05-138 or the Cyber Risk Profile or both, then the Sub-contractor may seek an adjustment to the contract price from the Prime Contractor for any associated increase or decrease in costs and the Sub-contractor may request an extension of time for compliance with such revised or amended DEFSTAN 05-138 or Cyber Risk Profile or both *provided always that* the Sub-contractor shall seek to mitigate the impact on time and cost to the extent which it is reasonably practicable to do so and *further provided that* such costs shall not be allowed unless they are considered to be appropriate, attributable to this Sub-contract and reasonable in all the circumstances.
- 5.4. The Sub-contractor shall not recover any costs and/or other losses under or in connection with this Condition where such costs and/or other losses are recoverable or have been recovered by the Sub-contractor elsewhere in this Contract or otherwise. For the avoidance of doubt this shall include but not be limited to the cost of implementing any upgrades or changes to any information system or electronic communications network whether in response to a Cyber Security Incident or otherwise, where the Subcontractor is

able to or has recovered such sums in any other provision of this Sub-contract or has recovered such costs and/or losses in other contracts between the Sub-contractor and the Prime Contractor or with other bodies.

**Annex H to SAL Apprentice Training****Dated: 17/10/2024****DEFCON 660: OFFICIAL-SENSITIVE SECURITY REQUIREMENTS<sup>6</sup>**

1. In this condition 'Information' means information recorded in any form disclosed or created in connection with the Contract.
2. The Contractor shall protect all Information relating to the aspects designated OFFICIAL-SENSITIVE as identified in the security aspects letter annexed to the Contract, in accordance with the official security conditions contained in the contract or annexed to the security aspects letter<sup>7</sup>.  
(o)
3. The Contractor shall include the requirements and obligations set out in clause 2 in any sub-contract placed in connection with or for the purposes of the Contract which requires disclosure of OFFICIAL-SENSITIVE Information to the subcontractor or under which any Information relating to aspects designated as OFFICIAL-SENSITIVE is created by the subcontractor. The Contractor shall also include in the sub-contract a requirement for the subcontractor to flow the requirements of this clause to its subcontractors and through all levels of the supply chain to the lowest level where any OFFICIAL-SENSITIVE Information is handled.

---

<sup>6</sup> Edition 12/15

<sup>7</sup> Annex C

**Annex I to SAL Apprentice Training**

**Dated: 17/10/2024**

**SAL ACKNOWLEDGMENT SHEET**

I confirm that I have read, understood, and will comply with:

I understand that the work on projects for **Apprentice Training Contract** is of a sensitive nature and will not discuss specifics of the work with anyone outside of the Project team.

I understand that failure to adhere to the Information Security management arrangements detailed in the above document or other documents referenced by it may result in disciplinary action being taken by the parent company; the revoking of my Security Clearance and site access and also potentially could lead to prosecution under the Official Secrets Act.

I understand that any questions regarding security should be directed to the Project Manager in the first instance.

Signed 

Name: David Bell

Date 14/11/2024

**Interim Process in support of DEFCON 658**

Jacqueline Barry (DES WpnsDM-CSI-Comrcl-1)  
Assistant Commercial Officer  
Defence Munitions  
Defence Equipment & Support,  
MOD Abbey Wood,  
Fir 1 #4110  
Bristol  
BS34 8JH

Email: jacqueline.barry111@mod.gov.uk

East Kilbride & District Group Training  
Association Ltd  
East Kilbride Training Centre  
Law Place, East Kilbride  
Glasgow  
G74 4PP

17/10/2024

**ITT REFERENCE:** 712133450-A – DM/00181  
**CYBER RISK PROFILE FOR ABOVE ITT:** Moderate

We refer to the above-mentioned ITT.

Please note that, for all contracts and relevant Sub-contracts which are assessed to have a Cyber Risk Profile of HIGH, clause 3.1.3 of DEFCON 658 is suspended until further notice but you must otherwise continue to comply fully with DEFCON 658 Edn 10/22. As part of this process, you must complete the Risk Assessment and Supplier Assurance Questionnaire using the interim process described in ISN 2021-05 and you must continue the flow down throughout the supply chain until the Cyber Risk Profile is no longer assessed to be HIGH.

With effect from 4 June 2021, for all contracts which are assessed to have a Cyber Risk Profile lower than HIGH (i.e. MODERATE, LOW or VERY LOW), the MOD confirms that the following clauses of DEFCON 658 shall operate as set out below until further notice by ISN and letter:

**Clauses 3.1.1 and 3.1.2:**

These clauses shall remain in effect for **all** MOD awarded contracts but, where a MOD awarded contract has a Cyber Risk Profile below HIGH and/or where a Sub-contract has a Cyber Risk Profile below HIGH, this clause is suspended for all relevant lower tier Sub-contracts which are awarded on or after 4 June 2021. Please see the diagrams attached at Appendix A to this letter which are provided for illustrative purposes.

**Clause 3.1.3:**

This clause is suspended for all contracts and Sub-contracts which are due to re-complete the CSM Supplier Assurance Questionnaire between 4 June 2021 and the end of the interim process.

**General:**



For the avoidance of doubt please note that:

- a. All other provisions of DEFCON 658 will continue to apply;
- b. In accordance with clause 3.1.9, DEFCON 658 should continue to be included in all relevant Sub-contracts. Strictly to the limited extent outlined above and in relation to Sub-contracts assessed to have a Cyber Risk Profile below HIGH, MOD is content for contractors to offer their Sub-contractors a suspension of the equivalent provisions to 3.1.1, 3.1.2 and 3.1.3 until the full Supplier Cyber Protection Service is available again;
- c. For Sub-contracts where the prime contract with MOD has been assessed to have a Cyber Risk Profile of MODERATE, LOW or VERY LOW, it is a matter for you to determine how best to ensure that cyber risk is appropriately managed until the full Supplier Cyber Protection Service is available again. However, contractors are expected to act reasonably and proportionately in relation to relevant Sub-contracts.

The Supplier Cyber Protection Service tool is expected to be delivered in the Summer of 2022 and the MOD will notify you by ISN and letter when you should recommence the use of the online tool.

At this point, MOD will also confirm the period within which:

- a. any annual renewals of CSM Supplier Assurance Questionnaires must be completed in order to be considered compliant with clause 3.1.3 of DEFCON 658; and
- b. Sub-contracts with a Cyber Risk Profile of MODERATE, LOW and VERY LOW must again comply with all of the obligations set out in clauses 3.1.1 and 3.1.2.
- c. This period is expected to be no less than 6 weeks, although may be longer depending on the period for which the Supplier Cyber Protection Service has been offline.

Signed on behalf of the MOD ....N Dewfall (DES WpnsDM-CSI-ComrcSCO)...

Please sign and date this letter below and return by post and email to the MOD Commercial Officer at the email address above to confirm receipt and acknowledge the provisions set out above.

Signed on behalf of the Contractor by



David Bell

General Manager & Company Secretary

East Kilbride & District Engineering Group Training Association Ltd

Date: 14/11/2024