CONTRACT ORDER FORM

This Contract Order Form is issued in accordance with the provisions of the Apprenticeship Training Provider Dynamic Marketplace (DMP) Agreement for the provision of Apprenticeship Training Services.

This contract will be for CCDE23A05 - Digital & Technology Solutions Professional Integrated Degree Level 6 Apprenticeship. Dated 02.11.2023.

The Supplier agrees to supply the Goods and/or Services specified below on and subject to the terms of this Contract.

For the avoidance of doubt this Contract consists of the terms set out in this Contract Order Form and the Contract Terms

Order Number	To be confirmed upon award
From	Sellafield Ltd ("Customer")
To	QA Ltd ("Supplier")

1. CONTRACT PERIOD

1.1	Commencement Date	Mobilisation Start Date: 7th November 2023 Service Delivery Start Date: 1st September 2024
1.2	Expiry Date (Apprenticeship programme completion date / End Point Assessment completion date)	31st August 2028

2. SERVICES REQUIRED

2.1	Services Required. APPRENTICESHIP TRAINING PROVIDER SERVICES / END POINT ASSESSOR SERVICES / BOTH. LOCATION APPRENTICESHIP TYPE AND SPECIFIC APPICABLE INSTITUTE FOR APPRENTICESHIPS STANDARD NUMBER OF STUDENTS	As outlined in the Call Off Contract Terms, Contract Schedule 2, Annex 1 – The Services

	CLASS BASED ADDITIONAL SERVICES	

3. CONTRACT PERFORMANCE

3.1	Required Apprenticeship Standard	ST0119 Digital and Technology Solutions Professional (integrated degree) Level 6

3.1	Quality Standards	Continued adherence to the relevant Institute for Apprenticeships industry standard. (www.instituteforapprenticeships.org/) Maintained ESFA registration and accreditation. General industry good practice

4. PAYMENT

4.1	Contract Charges	REDACTED TEXT under FOIA Section 43, Commercial Interests
4.2	Payment terms/Profile	Payment to be made in accordance with the current in force ESFA funding rules. Further additional terms in Annex 2 of Contract Schedule 3 As outlined in section 18 of Annex 1 – The Services
4.3	Customer billing address	Invoices should be submitted to: REDACTED TEXT under FOIA Section 40, Personal Information

5. LIABILITY AND INSURANCE

5.1	Suppliers limitation of Liability	In Clause 25 of the Contract Terms
5.2	Insurance	(Clause 26 of the Contract Terms): Professional Indemnity Insurance cover of £1 million any one claim. Public Liability Insurance cover of £1 million any one claim. Employers Liability insurance cover of £5 million any one claim.

6. OTHER CALL OFF REQUIREMENTS

Transitional Arrangements and Contract Management

1. TRANSITIONAL ARRANGEMENTS AND CONTRACT MANAGEMENT

1.1 Where required by Appendix A to Annex 1 of Contract Schedule 2 of the Contract Terms, the Supplier will be required to support the Transitional Services.

1.2 In providing support to such Transitional Services, the Supplier shall comply with the Transitional KPIs detailed in Annex 3 of Contract Schedule 2 of the Contract Terms.

1.3 Where the Supplier fails to meet the Transitional KPIs , pursuant to Clause 1.2, such failure being an (**"Intervention Cause"**), the Customer may give notice to the Supplier (**"Intervention Notice"**) giving details of the intervention and requiring a meeting between the Customer Representative and the Supplier Representative (**"Intervention Meeting"**) to discuss the Intervention Cause at a time and location specified by the Customer.

1.4 A failure to meet will the Transitional KPIs not give rise to Supplier Non-Performance (as defined at Clause 28 of the Contract Terms) save to the extent that the same cause has resulted in the Supplier otherwise failing to provide the Goods and/or Services in accordance with the Service Levels, or complying with its other obligations under this Contract, in which case the Customer's rights pursuant to this Clause 1 are without prejudice to the Customer's other rights under this Contract.

1.5 The Customers' and Supplier's overall objective in the Intervention Meeting shall be to prevent or mitigate the effects of, and (to the extent capable of being remedied) to remedy, the Intervention Cause and to avoid the occurrence of similar circumstances in the future.

1.6 In furtherance of this objective (but without diminishing the Supplier's responsibilities under this Contract), the parties agree that, following the Intervention Meeting, the Customer may undertake any one or more of the following actions:

(a) observe the conduct of and work alongside the Supplier Personnel to the extent that the Customer considers reasonable and proportionate having regard to the Intervention Cause;

(b) gather any information the Customer considers relevant in the furtherance of its objective;

(c) make recommendations to the Supplier as to how the Intervention Cause might be mitigated or avoided in the future; and/or

(d) take any other steps that the Customer reasonably considers necessary or expedient in order to mitigate or rectify the Intervention Cause.

1.7 The Supplier shall:

(a) work alongside, provide information to, co-operate in good faith with and adopt any reasonable methodology in providing the Services recommended by the Customer;

(b) ensure that the Customer has all the access it may require in order to carry out any actions that it has been agreed the Customer shall undertake;

(c) consult with the Customer in every instance where the Customer requests such consultation and consider in good faith

	any recommendations made by the Customer in the course of such consultations; (d) submit to such monitoring as the Customer considers reasonable and proportionate in respect of the Intervention Cause; and (e) implement any reasonable recommendations made by the Customer within the timescales given by the Customer. 1.8 Where the Supplier does not propose to follow recommendations made by the Customer pursuant to Clause 1.7, the Supplier shall, as soon as possible and in any event within forty eight (48) hours of such recommendations being made by the Customer: (a) inform the Customer which recommendation(s) the Supplier will not follow; (b) provide detailed reasons to the Customer as to the reasons why the Supplier will not follow such recommendations; and (c) provide alternative proposals to address and remediate the concerns raised by the Customer. 1.9 Within five (5) Working Days of the Supplier providing the information required pursuant to Clause 1.8, the Customer and the Supplier shall meet to discuss the Supplier's proposed approach to addressing and remediating the Customer's concerns. 1.10 The parties shall ensure that sufficiently senior representatives shall participate in any discussions that take place pursuant to Clause 1.9, and the parties shall act in good faith in the course of any such meeting to reach a solution satisfactory to both the Customer and the Supplier. 1.11 The Supplier shall be responsible for its own costs in connection with any action required by the Customer pursuant to this Clause 1. **2. CONTRACT ADMINISTRATION PLAN** 1.1 Within three (3) months of the Contract Commencement Date, a detailed contract administration plan (**"Contract Administration Plan"**) will be developed by the Supplier to ensure effective management, control and audit of the Supplier. The purpose of the Contract Administration Plan is to set out how the obligations of the Customer and the Supplier should be carried out effectively and efficiently by summarising the roles, responsibilities, authorities and limitations of the Key Personnel involved in managing the contract. The Contract Administration Plan will also cover continuous improvement, identification of efficiencies and innovative ways of working and enhancing delivery in relation to the Services. The Contract Administration Plan is intended to encourage a positive working practice between the Customer and the Supplier.
	Provision of Management Information **1. PROVISION OF MANAGEMENT INFORMATION** 1.1 The Supplier shall operate and maintain appropriate systems, processes and records to ensure that it can deliver timely and accurate Management Information. The Supplier shall provide timely, full, accurate and complete MI Reports which incorporates the data, in the correct format agreed between the Customer and the Supplier. 1.2 The Customer reserves the right to make changes to the data required or format of the MI Reports, any such change shall be communicated

	to the Supplier and the Customer shall specify the date from which the change is to be effective. 1.3 The Supplier shall provide the following management information (**"Management Information"**): • SLA Report; • Health & Safety; • Finance Reports; • Subcontractor Performance (including EPAOs); • KPI Report – KPIs will be reviewed monthly and a review of the KPI structure and content annually; • Health of Vocational and Education Programmes; • High Level overview of Apprentice Performances; and • Technical Query Progress. 1.4 The Customer may also require that the Supplier provides ad-hoc reporting such as heatmaps, gender, age set against criteria in relation to the Services.
	Security: **1. CIVIL NUCLEAR SECURITY REQUIREMENTS** 1.1 The Supplier acknowledges that it may have access to and/or hold SNI in connection with, or for purposes of complying with, its obligations under this Agreement and that the Customer will issue to it a "Security Aspects Letter" (**"SAL"**) in respect of such SNI. The Supplier acknowledges that Customer may update, amend and reissue the SAL from time to time. As a precondition to any obligation of the Customer (including payment) under this Agreement, the Supplier must execute the SAL (and any updated SAL) and return it to the Customer. 1.2 The Supplier shall at all times comply with the Official Secrets Acts 1911-1989, Nuclear Industries Security Regulations (NISR) 2003 and Section 79 (offence to intentionally or recklessly disclose) of the Anti-Terrorism, Crime and Security Act 2001 in connection with this Agreement. The Supplier acknowledges the importance of safeguarding SNI from disclosure, which could prejudice the security of nuclear sites and nuclear material on sites or in transportation (and that such disclosure could assist terrorists or others with malicious intent to attack or sabotage nuclear facilities or steal nuclear material) and understands the potentially serious consequences for its Employees and Sub-Contractors if they fail to ensure compliance by the Supplier with these requirements. The Supplier shall ensure that all its Employees and Sub-Contractors engaged in the performance of this Agreement are given notice of the relevance of this legislation and the potentially serious consequences of failure to comply with it. If directed by the Customer, the Supplier shall ensure that any Employee and Sub-Contractors shall sign a statement that they understand their obligations and are complying and will comply with them. 1.3 The Supplier shall implement and operate the procedures, policies and standards and all other requirements set out in the SAL (and any updated and amended SAL), including applying the required levels of Protective Security in respect of all SNI as defined in the SAL. The Supplier shall ensure that all documents, files and records are protected in accordance with the security related provisions of this Agreement and in accordance with the SAL.

1.4 The Supplier shall comply with all aspects of the Security Policy Framework (**"SPF"**), as set out in the SAL.

1.5 In complying with its obligations under this Agreement, the Supplier shall, at all times (including after completion of its obligations under this Agreement), comply with NISR 2003. As part of this obligation the Supplier shall ensure that all its employees and personnel engaged in the performance of this Agreement are given notice of NISR 2003 and shall report any breach or suspected breach of security (including any loss or compromise of SNI) to the Customer in accordance with the terms of the SAL.

1.6 The Supplier shall prevent any loss or compromise of SNI and shall protect it from deliberate or opportunist attack. The Supplier shall not, without the written consent of the Customer (which may be withheld in the Customer's absolute discretion), disclose this Agreement or any SNI to any person.

1.7 If the Supplier discovers or suspects that an unauthorised person is seeking or has sought to obtain information concerning any SNI, the Supplier shall forthwith notify the Customer.

1.8 The Supplier acknowledges and agrees that the Customer and ONR may at any time have access to and review and take copies of all information and/or documentation relating to the management of this Agreement (including standards, procedures and associated records), particularly those aspects relating to the security of SNI. This includes the Supplier ensuring the Customer can enter and inspect and have access to the assets and premises of the Supplier and Sub-Contractors, wherever located, if they are used for the purposes of or in connection with the performance of obligations under this Agreement. The Supplier acknowledges that there is no limit on such access or reviews, whether in terms of frequency, duration or otherwise, and the Supplier will fully co-operate in connection with such access and reviews.

1.9 The Supplier shall appoint a security manager to take responsibility for all aspects of its obligations under this Agreement which relate to security, including SNI (the **"Security Manager"**). The Supplier shall, prior to commencing its obligations under this Agreement, notify the Customer of the name, qualifications and experience of the proposed Security Manager. The Customer shall (in the Customer's absolute discretion) prior to contract award approve or otherwise the Security Manager. The Supplier shall not change an approved Security Manager without the prior written consent (in the Customer's absolute discretion) of the Customer. The Supplier shall ensure that the Security Manager implements and maintains an effective security regime to cover access, transmission, processing, storage and destruction of SNI.

1.10 The Customer may at any time request from the Supplier or any Employee or Sub-Contractor a "Statement of Compliance" in respect of the provisions of this Agreement (or any Sub-Contract), which relate to security of SNI and compliance with all aspects of the SAL. The Supplier shall provide or procure from its Employees and Sub-Contractors (as requested) a statement in the form set out in the SAL within 14 calendar days of the Customer's request.

1.11 The Supplier shall not:

(a) disclose the terms and conditions of this Agreement to any third party without the prior written consent of the Customer (which may be withheld in the Customer's absolute discretion). Communication of SNI within the Supplier's organisation must

be only where the recipient is authorised pursuant to the SAL, has not been expressly prohibited by the Customer, is an Employee and in each case needs to know that information for the performance of this Agreement;

(b) publicise its involvement with the Customer or this Agreement (including in any publicity literature or website or through the media or exhibition or symposium, or through scientific or technical papers or at any event attended by the public (whether organised by the Customer, a government body, or otherwise) without the prior written consent of the Customer (which may be withheld in the Customer's absolute discretion); or

(c) take any photographs or copies of SNI except to the extent necessary to comply with this Agreement.

1.12 The Supplier may not Sub-Contract any aspect of its obligations under this Agreement (or communicate with any potential Sub-Contractor relating to a potential Sub-Contract) without the prior written consent of the Customer (in the Customer's absolute discretion). Where the Supplier wishes to obtain the Customer's consent to subcontracting of its obligations under this Agreement (or communicating with a potential Sub-Contractor), the Contractor must notify the Customer of:

(a) the identity of the proposed Sub-Contractor;

(b) the proposed terms of Sub-Contract, which as a minimum, will require all Sub-Contractors at all levels of subcontracting to agree to terms equivalent to the terms of this Agreement;

(c) the scope of obligations proposed to be subcontracted;

(d) the arrangements for ensuring that all aspects of the Supplier's obligations relating to security of SNI and all requirements of the SAL will continue to be observed and maintained notwithstanding such subcontracting arrangements; and

(e) any other details required by the Customer.

1.13 The Customer may grant or withhold its consent to such subcontracting (or communication) on any basis and may attach conditions to any granted consent (including the execution of a SAL by any Sub-Contractors), in its absolute discretion.

1.14 In the event that the Supplier is in breach of its obligations under this Agreement relating to security of SNI or its obligations under the SAL or any secrecy or security obligation owed to the Crown or any other government body, the Customer may take any action it considers appropriate or necessary, including:

(a) notification of the appropriate authorities, including the ONR, the police or any other security agency;

(b) immediate suspension of the whole or any part of this Agreement's obligations and recommencement of such obligations;

(c) a requirement that specific persons or Sub-Contractors connected with such breach be removed from their involvement with the project and cease to have any access to the SNI;

(d) the return and/or evidenced destruction of SNI;

(e) the implementation of measures to protect and secure SNI; and/or

(f) termination of the Supplier's engagement under this Agreement in whole or in part.

1.15 The Customer shall have no liability to the Supplier for any action taken pursuant to Clause 1.14 and all consequences of such action shall be at the Supplier's cost.

1.16 All property, assets and information provided to the Supplier pursuant to this Agreement shall at all times remain the property of the Customer. Upon completion of its obligations under this Agreement, or at any other time on request of the Customer, the Supplier shall return all such property, assets, information and SNI to the Customer or in the case of SNI, to the extent specified by the Customer, provide evidence to the Customer that all SNI has been destroyed, in each case in a manner that does not contravene the requirements of this Agreement which relate to the security and does not contravene the SAL. To the extent any security related equipment has been loaned or used by the Supplier, the Supplier must ensure the safe return of such equipment in the condition specified by this Agreement.

1.17 The Supplier shall ensure that SNI created by or originating from the Supplier (or its Sub-Contractors) in connection with the performance of the Supplier's obligations under this Agreement shall become and remain the property of the Customer and shall not be subject to any restriction or otherwise. The Supplier shall (and shall ensure that its Sub-Contractors shall) take all steps and execute all documentation to ensure that the Customer can enjoy the full benefit of this Clause 1.17. Any samples, pattern, specifications, plans, drawings or any other documents issued by or on behalf of the Customer to the Supplier for the purposes of this Agreement shall remain the property of the Customer.

1.18 The Supplier shall provide to the Customer, upon request, records of which Employees have had access to SNI.

1.19 The Supplier shall not permit any change to the entities controlling it or its Sub-Contractors or any change to Key Employees or Sub-Contractor Key Personnel (as may be identified in the SAL) without the prior written consent of the Customer. The Supplier shall also notify the Customer of any changes in the behavioural or personal circumstances of Employees or personnel of Sub-Contractors to, the extent relevant to the matters set out in these terms and conditions and/or the requirements of the SAL. If such changes are likely to occur the Contractor shall inform the Customer at its earliest opportunity. The Customer shall, in its absolute discretion determine whether or not such change has an impact on the matters set out in these terms and conditions and/or the requirements of the SAL. If the Customer determines that there is such an adverse impact it may exercise any of the powers set out in Clause 1.14.

2. CYBER SECURITY

General Cyber Security Requirements

2.1 As a minimum, the Supplier shall, and shall procure that each of its Sub-Contractors and supply chain members performing services and/or works and/or supplying goods in connection with this Contract shall, obtain and maintain for the duration of the Contract Period, a Cyber Essentials Certificate (or equivalent certification and/or ISO 27001).

2.2 Not used

2.3 Prior to the commencement of the Services and, in any event, within 30 Working Days of the date of this Agreement, the Supplier shall provide to the Customer a Cyber Essentials Declaration for Supplier signed by a director of the Supplier.

2.4 Prior to the performance of any services and/or works and provision of goods by a Sub-Contractor, and in any event, within 3 months of the

date of this Agreement, the Supplier shall provide the Customer a copy of a Cyber Essentials Declaration for such Sub-Contractor signed by a director of such Sub-Contractor. Notwithstanding any other provision of this Agreement, the Supplier shall not appoint any Sub-Contractor in connection with this Agreement that has not provided a Cyber Essentials Declaration.

2.5 Throughout the Contract Period, on each anniversary of the first Cyber Essentials Declarations provided to the Customer pursuant to Clause 2.3, the Supplier shall deliver the Customer a renewed Cyber Essentials Declaration for the Supplier and, save where otherwise agreed by the Customer in its absolute discretion in accordance with Clause 2.1, for each Sub-Contractor and all supply chain members performing Services and/or works and/or supplying goods in connection with this Agreement, at the relevant time on each anniversary of the first applicable Cyber Essentials Declaration given by Supplier under Clause 2.3 and/or the relevant Sub-Contractor under its Sub-Contract.

2.6 If, following delivery of a Cyber Essentials Declaration by the Supplier and/or any Sub-Contractor in respect of certification obtained in accordance with Clause 2.1, the Supplier and/or Sub-Contractor is subsequently required to obtain certification in accordance with Clauses 2.10, 2.14 or 2.17 (as applicable) the Supplier and/or the relevant Sub-Contractor shall deliver to the Customer a further Cyber Essentials Declaration in respect of its certification obtained in accordance with Clauses 2.10, 2.14 or 2.17 as applicable, signed by a director of the Supplier and/or relevant Sub-Contractor (as appropriate) prior to the commencement of the part of the Services requiring the Supplier and/or the relevant Sub-Contractor to work with OS Information and/or SNI.

2.7 The Customer may, from time to time (acting reasonably), instruct the Supplier to provide, in respect of the Supplier itself, or to procure that a Sub-Contractor or other supply chain member that is performing Services and/or works and/or supplying goods in connection with this Agreement at the relevant time undertakes, a renewed Cyber Essentials Declaration. The Supplier shall comply with such instruction within a reasonable period and shall provide the renewed Cyber Essentials Declaration to the Customer.

2.8 If the Supplier fails to comply with any of Clauses 2.3, 2.4, 2.5, 2.11, 2.15 and/or 2.19 (as applicable), the Customer may take any actions it considers appropriate or necessary, including any or all of the following:

(a) immediate suspension of the whole or any part of the Supplier's obligations and recommencement of such obligations;

(b) a requirement that specific Sub-Contractors connected with such breach be removed from their involvement with the provision of the Services and cease to have any access to the OS Information and/or SNI;

(c) the withholding of and/or the requirement of the return and/or evidenced destruction of OS Information and/or SNI;

(d) the implementation of measures to protect and secure OS Information and/or SNI; and/or

(e) termination of the Supplier's engagement under this Contract in whole or in part in accordance with Clause 30 of the Contract Terms.

Cyber Security Requirements: Official Information

2.9 Where the Supplier will be required to possess and/or process and/or create Official Information and/or other sensitive and/or personal information on an Internet Connected System in the performance of its obligations under this Contract, clauses 2.10 to **Error! Reference source not found.** (inclusive) shall apply in addition to the General Cyber Security Requirements set out at clauses 2.1 to 2.8 (inclusive).

2.10 The Supplier acknowledges that the Customer requires, as a minimum standard, that the Supplier and all members of its supply chain working with Official Information to obtain and maintain, "Cyber Essentials" accreditation (or equivalent certification and/or ISO 27001) pursuant to the Cyber Essentials Scheme, at all times.

2.11 It shall be a condition precedent to the entitlement of the Supplier to receive any payment (or any further payment where a Cyber Essentials Certificate (or equivalent certification under ISO 27001) has expired and not been renewed) from the Customer under this Contract, that the Supplier shall obtain and maintain a valid Cyber Essentials Certificate (or equivalent certification and/or ISO 27001) for the duration of the Contract Period.

2.12 Not used

Cyber Security Requirements: Official-Sensitive Information

2.13 Where the Supplier will be required to possess and/or process and/or create OS Information on an Internet Connected System in the performance of its obligations under this Contract, Clauses 2.14 and 2.15 shall apply in addition to the General Cyber Security Requirements set out at clauses 2.1 to 2.8 (inclusive).

2.14 The Supplier acknowledges that the Customer requires, as a minimum standard, that the Supplier and all members of its supply chain working with OS Information to obtain and maintain, "Cyber Essentials Plus" accreditation pursuant to the Cyber Essentials Scheme (or equivalent and/or ISO 27001), at all times whilst they are in possession of and/or processing and/or creating OS Information on an Internet Connected System.

2.15 Where the Supplier is required, pursuant to clause 2.14, to obtain Cyber Essential Plus (or equivalent), the provision and maintenance of a valid Cyber Essentials Plus Certificate and/or ISO 27001 (or an equivalent accreditation approved by the Customer) for the Supplier without undue delay and in any event within 3 (three) months of receipt of request by the Customer to do so, is a condition precedent to the entitlement of the Supplier to receive any payment (or any further payment where a Cyber Essentials Plus Certificate or an equivalent accreditation approved by the Customer) has expired and not been renewed) from the Customer.

Cyber Security Requirements: Sensitive Nuclear Information (SNI)

2.16 Where the Supplier will be required to possess and/or process and/or create SNI on an Internet Connected System in the performance of its obligations under this Contract, Clauses 2.17 to 2.19 (inclusive) shall apply in addition to the General Cyber Security Requirements set out at clauses 2.1 to 2.8 (inclusive).

2.17 The Supplier acknowledges that the Customer requires, as a minimum standard, that the Supplier and all members of its supply chain working with SNI and/or the Customer's Data, to obtain and maintain "Cyber

Essentials Plus" accreditation (or equivalent and/or ISO 27001) pursuant to the Cyber Essentials Scheme and to comply with the Sellafield Additional CE+ Requirements set out in Part 2 to Appendix A, at all times whilst they are in possession of and/or processing and/or creating SNI on an Internet Connected System.

2.18 Not used

2.19 Where the Supplier is required, pursuant to clause 2.17, to obtain Cyber Essential Plus (or equivalent) and/or ISO 27001 and to comply with any Sellafield Additional CE+ Requirements, the provision and maintenance of a valid Cyber Essentials Plus Certificate and/or ISO 27001 (or an equivalent accreditation approved by the Customer) for the Supplier without undue delay and in any event within 3 (three) months of receipt of request by the Customer to do so, is a condition precedent to the entitlement of the Supplier to receive any payment (or any further payment where a Cyber Essentials Plus Certificate or an equivalent accreditation approved by the Customer) has expired and not been renewed) from the Customer.

2.20 It shall be a condition precedent to the entitlement of the Supplier to receive any payment (or any further payment where a Cyber Essentials Plus Certificate (or equivalent and/or ISO 27001) has expired and not been renewed) from the Customer under this Contract, that the Supplier shall obtain and maintain a valid Cyber Essentials Plus Certificate (or equivalent and/or ISO 27001) and comply with the Sellafield Additional CE+ Requirements for the duration of the Contract Period.

Non-EEA Nationals

2.21 The Supplier acknowledges that:

(a) prior to provision of access of information to a Non-EEA Employee, the Customer is required to inform the ONR of any Non-EEA Employees that may have access to OS Information and/or SNI (whether directly or indirectly); and

(b) the Supplier shall provide to the Customer the name, nationality, job title and an explanation of why such Non-EEA Employee needs access to SNI, for submission by the Customer to the ONR for approval;

(c) if such Non-EEA Employee is approved by the ONR, the Customer is required by the ONR to carry out the Customer's baseline security clearance checks to enable such Non-EEA Employee to have access to SNI; and

(d) the completion of the process for the approval of Non-EEA Employees set out in Clauses 2.21(a) to 2.21(c) can take up to 30 Working Days.

2.22 The Supplier shall promptly notify the Customer, by email to REDACTED TEXT under FOIA Section 40, Personal Information of any of its Non-EEA Employees that may have access to SNI (whether directly or indirectly) and, in any event, not less than 30 business days prior to the date when the Supplier intends to provide such Non-EEA Employee with SNI. The notification shall include such Non-EEA Employee's name, nationality, job title and an explanation of why such Non-EEA Employee needs access to SNI. Such Non-EEA Employees shall not have access to SNI until approval is given by the Customer.

2.23 If a Non-EEA Employee is approved by the ONR and passes the Customer's baseline security clearance checks, without prejudice to the

	Supplier's obligations in this Clause 1 such Non-EEA Employee may have access to SNI in accordance with the Customer's approval. 2.24 If a Non-EEA Employee is not approved by the ONR, or, is approved by the ONR but does not pass the Customer's baseline security clearance checks, the Supplier shall not permit such Non-EEA Employee access to SNI.
	Rights of Third Parties **1. RIGHTS OF THIRD PARTIES** 1.1 The NDA shall, pursuant to the Contracts (Rights of Third Parties) Act 1999, be entitled to enforce any of the Customer's rights under this Agreement and any term in this Agreement which directly or indirectly prevents or attempts to prevent the NDA from exercising those rights shall have no legal effect. 1.2 The Supplier acknowledges that its obligations under this Agreement benefit both the Customer and the NDA.
	Nuclear Installations Act **1. NUCLEAR INSTALLATIONS ACT 1965** 1.1 Pursuant to section 12(3A) of the Nuclear Installations Act 1965 (the **"Act"**), the Customer and the Supplier agree as follows: (a) Subject to the following, in the event of an occurrence involving nuclear matter as defined within section 7 of the Act, the Customer is liable to the Supplier for damage to the property of the Supplier and/or the property of the Supplier's Sub-Contractors or suppliers which is located on the Customer's Nuclear Licensed Site for the purposes of this Agreement. (b) The Customer's liability under this clause 1.1 is limited to liability for property damage as would otherwise exist if section 7(3) of the Act did not apply and claims under this contract for property damage shall be governed by the Act as if section 7(3) of the Act did not apply. (c) The Customer is not liable under this clause 1.1 unless and to the extent that the Supplier has: (i) notified the Customer and the NDA of the estimated value of the Supplier's plant, equipment and assets and any such plant, equipment and assets of its Sub-Contractors or suppliers brought onto the Customer's Nuclear Licensed Site on an annual basis for the purposes of this Agreement in accordance with the NDA's insurance renewal requirements; and (ii) where the estimated value of such property has changed by twenty per cent (20%) or more during any one (1) year, notified the Customer and the NDA of the amount of such change. (d) The Customer's liability under this clause 1.1 is limited to the market value of the property notified in writing in accordance with the above. (e) The Customer is liable under this Clause 1.1 to the extent that the occurrence involving nuclear matter was attributable to any act or omission of the Supplier or any employee, servant or agent of the Supplier, or the Supplier's Sub-Contractor or any employee, servant or agent of the Supplier's Sub-Contractor done with the intent

	to cause injury or damage or done with reckless disregard for the consequences of the act or omission. 1.2 For the avoidance of doubt, nothing in this Agreement is or shall be deemed to be an agreement for the Supplier to incur liability under Section 12(3A) of the Act.
	Employee Transfers **1. PENSIONS** 1.1 Where as a result of entry into this contract, this contract and other contracts as a Series of Contracts or any Sub-Contract, the employment of any Protected Employee transfers to the Supplier, a Sub-Contractor or any Third Party (the **"Transferee Employee"**) and following the transfer of employment such Protected Employee continues to undertake wholly or mainly Authority Facing Works, the Supplier complies with, and procures that any Sub-Contractor or Third Party (as appropriate) (being the **"Transferee Employer"**) complies with the following provisions: (a) ensures that on or before the date of transfer of employment the Transferee Employer has established or become a participant in a pension scheme which has been certified by the Government Actuary's Department (**"GAD Certified Pension Scheme"**) as providing sufficient benefits to enable the NDA to satisfy itself that its duties and obligations under Part 4 of Schedule 8 of the Energy Act 2004 have been met, and complying fully with the Fair Deal on Staff Pensions issued by HM Treasury in June 1999, including the supplementary guidance issued by HM Treasury in June 2004 concerning bulk transfer payments; (b) ensures that on or before the date of transfer of employment each Protected Employee is enrolled as a member of the GAD Certified Pensions Scheme; (c) does and does not omit to do any such other thing which the NDA determines to be necessary to enable the NDA to satisfy itself that its duties and obligations in respect of the Protected Employees under Schedule 8 of the Energy Act 2004 are met; (d) maintains for the duration of this contract, Series of Contracts or Sub-Contract a record of those Protected Employees undertaking wholly or mainly Authority Facing Work; and (e) complies with the NDA's policies for the provisions of pensions within the nuclear industry. 1.2 In the event of any breach of the undertakings or other obligations set out in this Clause 1, where the Supplier is the Transferee Employee the Supplier does, and where the Supplier is not the Transferee Employee the Supplier ensures that the Transferee Employee does, all things reasonably necessary, as directed by the NDA, to restore the rights and benefits of such Protected Employees so as to enable the NDA to satisfy itself that its duties and obligations under Schedule 8 of the Energy Act 2004 are, and continue to be met.

In the event of any conflict between (i) The terms and conditions of Commercial Agreement RM6102 and; (ii) the Customer's Appendices C to G, the order of precedence is (i), (ii).

FORMATION OF CONTRACT

By signing and completing this Contract Order Form the Supplier and the Customer agree to enter into a binding contract governed by the terms of this Contract Order Form and the attached terms and conditions.

For and on behalf of the Supplier:

Name and Title	REDACTED TEXT under FOIA Section 40, Personal Information
Date	03.11.2023

For and on behalf of the Customer:

Name and Title	REDACTED TEXT under FOIA Section 40, Personal Information
Date	09.11.2023

APPENDIX A

PART 1

FORM OF CYBER ESSENTIALS DECLARATION

Cyber Essentials Declaration

I confirm that [insert name of Supplier/Subcontractor] complies with the following with regard to the provision of the Services in connection with this Contract:

a) Are accredited [Cyber Essentials] [Cyber Essentials Plus] [Delete as appropriate]in respect of the Supplier's business activities that were agreed with the Customer in advance of obtaining such accreditation [Delete if not applicable (i.e. where limb (c) applies)];

b) Are accredited with an equivalent scheme to [Cyber Essentials] [Cyber Essentials Plus] [Delete as appropriate] and have received approval from the Customer that the equivalent accreditation is acceptable [Delete if not applicable (i.e. where limb (b) applies)];

c) All personnel will only be using business issued devices covered by the [Cyber Essentials certificate] [Cyber Essentials Plus] [approved equivalent accreditation] [Delete as appropriate];

d) Are compliant with the Sellafield Additional CE+ Requirements [delete as appropriate].

Please attach the following:

- Copy of your Cyber Essentials Certificate or Cyber Essentials Plus Certificate or approved equivalent accreditation (together with written approval of the equivalent accreditation by the Customer) [delete as appropriate];

- If the [Cyber Essentials Certificate] [Cyber Essentials Plus certificate] OR [approved equivalent accreditation] does not cover the whole company, confirmation that it will cover all who are working / will be working on the provision of the Services [delete as appropriate];

- Details of the measures you take to comply with the Sellafield Additional CE+ Requirements [delete as appropriate];

- Details of the disk encryption software installed on the computers.

Signed: Signature ……

for and on behalf of …… [insert name of Supplier/Subcontractor]

Full name: ……
Date: ……