[redacted]

NHS Shared Business Services

Service Level Agreement (Order Form)

Framework details

Title: Internal and External Audit, Counter Fraud and Financial Assurance Services
Reference: [redacted]
Contract Duration: 16th November 2020
End Date: 15th November 2024
NHS SBS Contacts: [redacted]

Oder Form details

This Order Form is between the following parties and in accordance with the Terms and Conditions of the Framework Agreement.

Period of the Agreement	Effective Date	*27/11/23*	Expiry Date	*31/03/2024*
Extension		This Contract can be extended by the Authority up to 12 months by giving the Supplier 30 days prior written notice before its Expiry.		

Unless otherwise agreed by both parties, this Order Form will remain in force until the expiry date agreed above. If no extension/renewal is agreed and the customer continues to access the supplier's services, the terms of this agreement shall apply on a rolling basis until the overarching Framework expiry date.

Supplier Order Form Signature panel

The "Supplier"	
Name of Supplier	**MIAA (A shared service hosted by Liverpool University Hospitals NHS FT)**
Lot Awarded under	**Lot 2 - Provision of Internal Audit Services**
Name of Supplier Authorised Signatory	[redacted]
Job Title of Supplier Authorised Signatory	**Digital Director**
Address of Supplier	**MIAA Regatta Place Summers Road Brunswick Business Park Liverpool L3 4BL**
Signature of Authorised Signatory	

Authority Order Form Signature panel

The "Authority"	
Name of Authority	NHS England
Name of Authority Authorised Signatory	
Job Title	**Deputy CFO**
Contact Details email	[redacted]
Address of Authority	7 - 8 Wellington Place Leeds West Yorkshire LS1 4AP
Signature of Authority Authorised Signatory	

This service level agreement shall remain in force regardless of any change of organisational structure to the above named authority and shall be applicable to any successor organisations as agreed by both parties.

PLEASE RETURN THE FINAL SIGNED COPY OF THIS DOCUMENT TO:
[redacted]

[redacted]

Table of Contents

1. Agreement Overview
2. Goals & Objectives
3. Stakeholders
4. Periodic Review
5. Service Requirements
    a. Services Provided
    b. DBS
    c. Price / Rates
    d. Sub-contracting
    e. Management Information
    f. Invoicing
    g. Cancellation
    h. Complaints/Escalation Procedure
    i. Termination
6. Other Requirements
    a. Variation to Standard Specification
    b. Other Specific Requirements

1. Agreement Overview

This Agreement represents an Order Form between *MIAA (a shared service hosted by Liverpool Univeristy Hospital NHS FT)* and *NHS England* for the provision of Internal and External Audit, Counter Fraud and Financial Assurance Services. This Agreement remains valid until superseded by a revised agreement mutually endorsed by both parties. This Agreement outlines the parameters for all Internal and External Audit, Counter Fraud and Financial Assurance Services covered as they are mutually understood by the primary stakeholders.

The Framework terms and conditions (including the specification of service) will apply in all instances, unless specifically agreed otherwise by both parties within this document.

2. Goals & Objectives

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent Internal and External Audit, Counter Fraud and Financial Assurance Services to the Authority by the Supplier. The **goal** of this Agreement is to obtain mutual agreement for Internal and External Audit, Counter Fraud and Financial Assurance Services provision between the Supplier and Authority.

The **objectives** of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to the customer.

3. Stakeholders

The primary stakeholders from the Supplier and the Authority will be responsible for the day-to-date management of the Agreement and the delivery of the service. If different from the Authorised Signatory details listed on page 1 of this Agreement, please provide the names of the **primary stakeholders** associated with this Order Form.

Supplier Contact: [redacted]

Authority Contact: [redacted]

4. Periodic Review

This Agreement is valid from the **Effective Date** outlined herein and is valid until the **Expiry Date** as agreed. This Agreement should be reviewed as a minimum once per financial year; however, in lieu of a review during any period specified, the current Agreement will remain in effect.

5. Service Requirements

A. Services Provided

Please detail the Lot(s) and Services that will be provided by the Supplier to the Authority

This Contract is for the provision of Services under **Lot 2 - Provision of Internal Audit Services**

The Supplier will supply the Services to the Authority under the above Lot, as set out the Specification (Annex A), in accordance with the terms and conditions of this Contract.

In performing the Services, the Supplier shall meet, and time is of the essence as to, any performance dates specified in the Specification.

In supplying the Services, the Supplier shall:

(a) perform the Services with the highest level of care, skill and diligence in accordance with best practice in the Supplier's industry, profession or trade;

(b) co-operate with the Authority in all matters relating to the Services, and comply with all instructions of the Authority;

(c) appoint or, at the request of the Authority, replace without delay a manager, who shall have authority to contractually bind the Supplier on all matters relating to the Services. This person shall be the Supplier's representative;

(d) only use personnel who are suitably skilled and experienced to perform the tasks assigned to them, and in sufficient number to ensure that the Supplier's obligations are fulfilled;

(e) ensure that it obtains, and maintains all consents, licences and permissions (statutory, regulatory, contractual or otherwise) it may require and which are necessary to enable it to comply with its obligations in the Contract;

(f) ensure that the Services and/ or deliverables shall conform in all respects with the service description set out in the Specification and that the deliverables shall be fit for any purpose that the Authority expressly or impliedly makes known to the Supplier;

(g) provide all equipment, tools and other items required to provide the Services;

(h) ensure that all materials, standards and techniques used in providing the Services are of the best quality and are free from defects in workmanship, installation and design;

(i) comply with all applicable laws, statutes, regulations from time to time in force;

(j) not do or omit to do anything which may cause the Authority to lose any licence, authority, consent or permission on which it relies for the purposes of conducting its business; and

(k) notify the Authority in writing immediately upon the occurrence of a change of control of the Supplier.

B. DBS

The Authority should detail the level of DBS check requirement

1. Supplier Personnel shall be subject to pre-employment checks that include, as a minimum: verification of identity, employment history, unspent criminal convictions and right to work, as detailed in the HMG Baseline Personnel Security Standard (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard), as may be amended or replaced by the Government from time to time.

2. The Supplier shall agree on a case by case basis which Supplier Personnel roles which require specific government National Security Vetting clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Authority Data.

3. The Supplier shall prevent Supplier Personnel who have not yet received or are unable to obtain the security clearances required by this Clause 'D' (Staff Vetting) from accessing systems which store, process, or are used to manage Authority Data, or from accessing Authority premises, except where agreed with the Authority in writing.

4. All Supplier Personnel that have the ability to access Authority Data or systems holding Authority Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Authority in writing, this training must be undertaken annually.

5. Where Supplier Personnel are granted the ability to access Authority Data or systems holding Authority Data, those Supplier Personnel shall be granted only those permissions necessary for them to carry out their duties.

[redacted]

When staff no longer need such access or leave the organisation, their access rights shall be revoked within one (1) Business Day.

C. Price/Rates

Standard supplier pricing and rates are included within the pricing schedule. Please detail any discounts, volume arrangements or variations from the standard rates.

Each Audit will cost [redacted]

The number of Audits carried out will be dependent on a number of factors including the ability to schedule audits with the relevant NHS Trusts. [redacted]

The contract will therefore be capped at a value of **£135,000**

D. Sub-contracting

Subcontracting of services by Suppliers is allowed, both to Framework suppliers and to non-Framework suppliers. Any Supplier sub-contracting will be fully responsible for ensuring standards are maintained in line with the framework and this Order Form.

N/A

E. Management Information (MI)

Suppliers should provide Management Information as standard on a monthly basis. Authoritys should detail any additional management information required and the frequency of provision here.

Suppliers should provide a progress update against their delivery plan each week until all audits are complete, and reports are issued. If deemed appropriate and agreed by the Authority, progress updates may reduce in frequency to fortnightly.

F. Invoicing

Please detail any specific invoicing requirements here

1. The Authority shall issue a Purchase Order to the Supplier in respect of any Services to be supplied to the Authority under this Contract. The Supplier shall comply with the terms of such Purchase Order as a term of this Contract. For the avoidance of doubt, any actions or work undertaken by the Supplier under this Contract prior to the receipt of a Purchase Order covering the relevant Services shall be undertaken at the Supplier's risk and expense and the Supplier shall only be entitled to invoice for Services covered by a valid Purchase Order.

2. The Supplier must be in Receipt of a valid Purchase Order Number before submitting an invoice. All invoices should be sent, quoting that number to the address given on the purchase order. To avoid delay in payment it is important that the invoice is compliant and that it includes an item number (if applicable) and the details (name and telephone number) of the Authority contact. Non-compliant invoices will be sent back to the Supplier, which may lead to a delay in payment.

3. Any queries regarding outstanding payments should be directed to the Authority's Accounts Payable section by email at financialaccounts@nhs.net.

4. Invoices should clearly quote the purchase order number, be addressed to NHS England, T56 Payables A125 PO Box 312 Leeds LS11 1HP and be sent as a PDF attachment by email to the following email address: sbs.apinvoicing@nhs.net (one invoice per PDF) and emails must not exceed 10Mb and quote, 'T56 Invoice Scanning' in subject line or alternatively invoices can be sent via post to the above address.

5. In consideration of the supply of Services by the Supplier, the Authority shall pay the Supplier the invoiced amounts no later than 30 days after Receipt of a valid and undisputed invoice which includes a valid Purchase Order Number. The Authority may, without prejudice to any other rights and remedies under this Contract withhold or reduce payments in the event of unsatisfactory performance.

6. [redacted]

[redacted]

7. If there is a dispute between the Parties as to the amount invoiced, the Authority shall pay the undisputed amount. The Supplier shall not suspend the supply of the Services unless the Supplier is entitled to terminate this Contract. Any disputed amounts shall be resolved through the Dispute Resolution Procedure detailed in section 'H' (Complaints/Escalation Procedure), below, of this SLA.

8. If any sum of money is recoverable from or payable by the Supplier under this Contract (including any sum which the Supplier is liable to pay to the Authority in respect of any breach of the Contract), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Supplier under this Contract or under any other agreement or contract with the Authority. The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Authority in order to justify withholding payment of any such amount in whole or in part.

G. Cancellations

Please detail anything agreed with the supplier around cancellations.

H. Complaints/Escalation Procedure

Please detail any requirements regarding this

1. Any dispute between the Authority and the Supplier shall be dealt in accordance with the Dispute Resolution Procedure.

2. For the avoidance of doubt, the entirety of Clause 22 of Schedule 2 of this Contract shall be deemed not to apply and be deleted in its entirety from this Contract.

3. If there is a dispute in relation to this Contract, the Party raising the dispute shall serve a Dispute Notice setting out the details of the dispute. The Parties shall then attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with this Contract and such efforts shall involve the escalation of the dispute to an appropriately senior representative of each Party.

4. If the dispute cannot be resolved by the Parties within one month of the date of the Dispute Notice (being the date it was received) either Party may exercise any remedy it has under applicable law. For the avoidance of doubt, neither Party shall be prevented by this Dispute Resolution Procedure from commencing court proceedings more quickly if it is necessary to comply with a limitation period or if it is necessary to seek an urgent remedy.

5. The obligations of the Parties under this Contract shall not cease, or be suspended or delayed by the reference of a dispute to any dispute resolution process and the Supplier shall, and shall procure that all Staff shall comply fully with the requirements of this Contract at all times.

6. In relation to any such legal remedies or proceedings the Parties irrevocably agree that the Courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Contract or its subject matter or formation (including non-contractual disputes or claims).

7. For the avoidance of doubt, the entirety of Clause 30.10 of Schedule 2 of this Contract shall be deleted in its entirety and replaced with the following new Clause: "30.10 *The Parties irrevocably agree that the courts of England and Wales shall have exclusive jurisdiction to settle any Dispute or claim that arises out of or in connection with this Contract or its subject matter*."

I. Termination

Standard requirements are provided below as an example but may be amended to reflect local requirements.

Persistent failure by the Contractor to meet the agreed service levels as specified within the SLA may lead to the Contract being terminated or alternative Contractor(s) being appointed by the Authority to maintain levels of service

Prior to termination the complaints and escalation procedure should be followed to attempt to resolve any issue. Should suitable resolution not be achieved, the Authority will be allowed to terminate the SLA immediately.

[redacted]

The Authority may terminate this Contract forthwith in whole or in part by issuing a Termination Notice to the Supplier at any time on 30 days' written notice.

J. Location(s) at which the Services are to be provided:

The Services will be delivered to the health and social care entities remotely (i.e. NHS Foundation Trusts and CSUs) as directed by the Authority from time to time in accordance with the engagement process

The Supplier shall not be entitled to charge expenses to the Authority.

7. Other Requirements

Please list and agree the key requirements of the service

A. Data Protection Impact Assessment

The Supplier shall, at its own cost, participate and provide full co-operation for the completion of any Data Protection Impact Assessments conducted by the Authority relating to the Services and any related deliverables, such participation and co-operation shall include updating the Data Protection Impact Assessment following any variation agreed in writing between the Parties.

B. Variation to Standard Specification

Please list any agreed variations to the specification of requirements

None

C. Other Specific Requirements

Please list any agreed other agreed requirements

SUPPLEMENTAL AND/OR ADDITIONAL CLAUSES

The Parties agree to the inclusion of the following supplemental clauses:

1. **Anti-Slavery**

    a. The Supplier shall (i) comply with all relevant Law and Guidance and shall use Good Industry Practice to ensure that there is no slavery or human trafficking in its supply chains; and (ii) notify the Authority immediately if it becomes aware of any actual or suspected incidents of slavery or human trafficking in its supply chains.

    b. The Supplier shall at all times conduct its business in a manner that is consistent with any anti-slavery Policy of the Authority and shall provide to the Authority any reports or other information that the Authority may request as evidence of the Supplier's compliance with this requirement and/or as may be requested or otherwise required by the Authority in accordance with its anti-slavery Policy.

2. **Corporate Social Responsibility**

    a. The Supplier shall:

        i. comply, and procure that all Staff comply with all CSR Laws;

        ii. require its Sub-contractors and any person under its control, to comply with all CSR Laws;

        iii. adopt, and procure that its Sub-contractors and any person under its control adopt, written corporate and social responsibility policies that set out values for relevant activity and behaviour equivalent to those set out in the CSR Policies (including, without limitation, addressing the impact on employees, clients, stakeholders, communities and the environment of the Supplier's business activities); and

        iv. notify the Authority in the event that the Supplier's or its Sub-contractors' corporate and social responsibility policies conflict with, or do not cover the same subject matter in an equivalent level of detail as is in, the CSR Policies.

3. **IR35**

    a. This Contract constitutes an agreement for the provision of services. Where the Supplier (or its subcontractor) have included one or more people that are non-permanent members of staff that are not on the Supplier's (or its subcontractor) payroll ("**Contractor(s)**") to fulfil its service obligations under this Contract, the Supplier shall be fully responsible for and shall indemnify the Authority for:

        i. any proceedings, claims or demands by any third party (including specifically, but without limitation, HMRC and any successor, equivalent or related body pursuant to the IR35 legislation and/or any of the provisions of Income Tax Regulations);

        ii. any income tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with either the performance of the services or any payment or benefit received by the Contractor in respect of the services, where such recovery is not prohibited by law; and

        iii. all reasonable costs, expenses and any penalty, fine or interest incurred or payable by the Authority in connection with or in consequence of any such liability, deduction, contribution, assessment or claim.

    b. The Authority may at its option satisfy such indemnity (in whole or in part) by way of deduction from payments due to the Supplier.

    c. The Supplier warrants that it is not, nor will it prior to the cessation of this Contract, become a managed service company, within the meaning of section 61B of the Income Tax (Earnings and Pensions) Act 2003.

    d. The Supplier shall monitor the provision of the services and notify the Authority where it considers that the activity of the Authority may impact the Suppliers' (or its Sub-contractor) IR35 assessment in relation to the Contractors.

[redacted]

4. Protection of Personal Data

a. As of the Commencement Date, it is accepted there is no Processing of Personal Data involved under this Contract. It is agreed that each Party shall be responsible for ensuring Data Protection compliance in accordance with the Data Protection Legislation, in relation to its Processing of any Personal Data under this Contract. Should the Data Processing position change, (as there may be further services where the Authority is the Controller and the Supplier is the Processor, for example), the Parties acknowledge that the only Personal Data which may be shared under this Contract will be set out in the data table at Annex B (the Data Protection Protocol), which shall be issued as an addendum. Further, where it is agreed that processing shall take place and such addendum is issued, paragraph 2.2 of Schedule 3 and the provisions of the Data Protection Protocol, namely clauses 1.1 to 1.17 (Data protection) of Annex B of this Contract, must be complied with by the Parties as a term of this Contract.

b. For the avoidance of doubt, the Supplier shall ensure it is familiar with the Data Protection Legislation and any obligations it may have under such Data Protection Legislation and shall comply with such obligations.

c. The Supplier shall

i. at all times comply with any information governance requirements and/or processes as may be set out in the Specification and Tender Response Document; and

ii. comply with any new and/or updated requirements, Guidance and/or Policies notified to the Supplier by the Authority from time to time (acting reasonably) relating to the Processing and/or protection of Personal Data.

d. The Parties acknowledge that Clauses 2.4.1 and 2.4.2 of Schedule 3 shall be deemed to have been deleted and replaced with the Cyber Security Requirements.

5. Data Protection Impact Assessment Delivery and Assistance

a. Without limitation to the obligations as set out in the Data Protection Protocol, the Supplier shall provide a draft DPIA prior to contract award.

b. The Supplier shall update the DPIA to be complete for the agreed deliverables and meeting all Law, prior to the Commencement Date of the Contract. The Supplier shall be responsible for updating the DPIA at each material change of the Services and following any variation.

6. Quality Assurance Standards

The following quality assurance standards shall apply, as appropriate, to the provision of the Services:

a. The Supplier warrants and represents that it has complied with and throughout the Term will continue to comply with the Cyber Security Requirements.

b. The Supplier shall provide evidence that they have completed a DSP Toolkit submission 2019-20, or an equivalent assessment. From the Commencement Date, and throughout the Term, the Supplier should remain registered with the DSP Toolkit system (or any replacement to such system), or an equivalent.

c. The Supplier shall abide by the terms and guidance as detailed in and provided by the DSP Toolkit system. The Supplier shall maintain good information governance standards and practices that meet or exceed the DSP Toolkit standards required of its organisation type.

d. The Supplier shall from the Commencement Date, and throughout the Term should have the following accreditations or be able to demonstrate systems that their company operates systems/processes equivalent to such standards. The Supplier should supply copies of their accreditation certificates or evidence of their equivalent operating systems:

- BS EN ISO 9001
- Cyber Essentials+

7. Publicity and Branding

a. The Supplier shall not:

i. make any press announcements or publicise this Contract or its contents in any way; or

ii. use the Authority's name or brand in any promotion or marketing or announcement of orders,

without the prior written consent of the Authority.

b. Each Party acknowledges to the other that nothing in this Contract either expressly or by implication constitutes an endorsement of any products or services of the other Party (including the Services) and each Party agrees not to conduct itself in such a way as to imply or express any such approval or endorsement.

8. Non-solicitation

a. Except in respect of any transfer of Authority staff pursuant to the TUPE obligations in this Contract, the Supplier shall not (except with the prior written consent of the Authority) directly or indirectly solicit or entice away (or attempt to solicit or entice away) from the employment of the Authority any person employed or engaged by the Authority in the provision of the Services or in the receipt of the Services at any time during the Term or for a further period of six (6) months after the termination of the Contract other than by means of a national advertising campaign open to all comers and not specifically targeted at any of the Authority staff.

b. If the Supplier commits any breach of this specific Clause 8 (Non-solicitation), it shall, on demand, pay to the Authority a sum equal to six month's basic salary or the annual fee that was payable by the Authority to that employee, worker or independent contractor, plus the recruitment costs incurred by the Authority in replacing such person.

9. Assignment of Intellectual Property Rights in deliverables, materials and outputs

a. The Supplier confirms and agrees that all Intellectual Property Rights in and to the deliverables, material and any other output developed by the Supplier as part of the Services, in accordance with the Specification and Tender Response Document (including any reports) shall be owned by the Authority. The Supplier hereby assigns with full title guarantee by way of present and future assignment all Intellectual Property Rights in and to such deliverables, material and other outputs. The Supplier shall ensure that all Staff assign any Intellectual Property Rights they may have in and to such deliverables, material and other outputs to the Supplier and that such Staff absolutely and irrevocably waive their moral rights in relation to such deliverables, material and other outputs. This Clause '9' (Assignment of Intellectual Property Rights in deliverables, materials and outputs) shall continue notwithstanding the expiry or earlier termination of this Contract.

b. The product of the Supplier work may include advice or drafting suggestions or other documented contributions towards documents/ reports to be issued by the Authority in the Authority's own name without reference to the Supplier, which will be the Authority's and for which the Authority alone will be responsible. The Supplier will not assert any rights in or over any such documents/ reports prepared by the Authority.

10. Third party software

a. The following requirements shall take priority above all terms, conditions and specifications set out in this Contract (including without limitation any embedded documents and terms), and the Supplier shall ensure that the software licences meet and conform with the following requirements:

i. The Authority shall be entitled, free of charge, to sub licence the software to any contractor and/or Sub-contractor of the Authority who is working towards and/or is providing services to the Authority.

ii. The Authority's role as national information and technology partner to the NHS and social care bodies involves the Authority buying services for or on behalf of the NHS and social care entities. Nothing in the licences for any of the software shall have the effect of restricting the Authority from discharging its role as the national information and technology partner for the health and care system, which includes the ability of the Authority to offer software and services to the NHS and social care entities. Specifically, any software licensing clause prohibiting 'white labelling', 'provision of outsourcing services' or similar, shall not be interpreted as prohibiting the Authority's services.

iii. The Authority shall be entitled to deploy the software at any location from which the Authority and/or any contractor and/or Sub-contractor of the Authority is undertaking services pursuant to which the software is being licenced.

iv. Any software licenced to the Authority on a named user basis shall permit the transfer from one user to another user, free of charge provided that the Supplier is notified of the same (including without limitation to a named user who is a contractor and/or Sub-contractor of the Authority).

v. The Supplier shall ensure that the Authority shall be entitled to assign or novate all or any of the software licences free of charge to any other central government entity, by giving the licensor prior written notice.

vi. The Supplier shall notify the Authority in advance if any software or service permits the Supplier or any third party remote access to the software or systems of the Authority.

vii. Where the Supplier is responsible for the calculation of the appropriate number of users for software, and it is later shown there is a shortfall of licences, the Supplier shall be responsible for all costs of the Authority.

11. Force majeure

a. For the avoidance of doubt, the COVID-19 pandemic shall not constitute a Force Majeure Event under the terms of this Contract.

12. Change Control Process

a. Any changes or variations to this Contract, including to the Services, may only be agreed in accordance with the Change Control Process set out in Annex C.

For the purposes of incorporation of Schedule 4 (Definitions and Interpretations) into this Contract, the following definitions shall be added (and where such terms are already defined, such definitions shall be replaced with the corresponding definitions below):

"Authority Data"	means the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any Authority's Confidential Information, and which: i) are supplied to the Supplier by or on behalf of the Authority; or ii) the Supplier is required to generate, process, store or transmit pursuant to this Contract; or iii) any Personal Data for which the Authority is the Controller;
"CSR Policies"	means the Authority's policies, including, without limitation, anti-bribery and corruption, health and safety, modern slavery, the environmental and sustainable development, equality and diversity, and any similar policy notified to the Supplier by the Authority from time to time, and "CSR Policy" shall mean any one of them;
"CSR Laws"	means Laws relating to corporate social responsibility issues (e.g. anti-bribery and corruption, health and safety, the environmental and sustainable development, equality and diversity), including but not limited to the Modern Slavery Act 2015, the Public Services (Social Value) Act 2012, the Public Contracts Regulations 2015 and Article 6 of the Energy Efficiency Directive 2012/27/EU, from time to time in force;
"Change Control Process"	means the change control process, referred to in this SLA and in accordance with Annex C;

[redacted]

"Comparable Supply"	means the supply of services to another Authority of the Supplier that are the same or similar to any of the Services;
"Cyber Security Requirements"	means: a) compliance with the DSP Toolkit or any replacement of the same; and b) any other cyber security requirements relating to the Services notified to the Supplier by the Authority from time to time;
"DSP Toolkit"	means the data security and protection toolkit, an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards and supports key requirements of the UK GDPR, which can be accessed from https://www.dsptoolkit.nhs.uk/, as may be amended or replaced by the Authority or the Department of Health and Social Care from time to time;
"Data Protection Legislation"	means applicable legislation protecting the fundamental rights and freedoms of individuals, in respect of their right to privacy and the processing of their personal data, as amended from time to time, including Regulation (EU)_2016/679 as transposed into the United Kingdom's national law by the operation of section 3 of the EU (Withdrawal) Act 2018 (and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019; 'the UK General Data Protection Regulation' ("UK GDPR") and the Data Protection Act 2018) and the Privacy and Electronic Communications Regulations 2003, together with decisions, guidelines, guidance notes and codes of practice issued from time to time by courts, data protection authorities and other applicable Government authorities;
"Dispute Resolution Procedure"	means the process for resolving disputes as set out in section 'H' (Complaints/Escalation Procedure) of this SLA;
"Force Majeure Event"	means any event beyond the reasonable control of the Party in question to include, without limitation: (a) war including civil war (whether declared or undeclared), riot, civil commotion or armed conflict materially affecting either Party's ability to perform its obligations under this Contract; (b) acts of terrorism; (c) flood, storm or other natural disasters; (d) fire; (e) unavailability of public utilities and/or access to transport networks to the extent no diligent supplier could reasonably have planned for such unavailability as part of its business continuity planning; (f) government requisition or impoundment to the extent such requisition or impoundment does not result from any failure by the Supplier to comply with any relevant regulations, laws or procedures (including such laws or regulations relating to the payment of any duties or taxes) and subject to the Supplier having used all reasonable legal means to resist such requisition or impoundment; (g) compliance with any local law or governmental order, rule, regulation or direction applicable outside of

		England and Wales that could not have been reasonably foreseen; (h) industrial action which affects the ability of the Supplier to provide the Services, but which is not confined to the workforce of the Supplier or the workforce of any Sub-contractor of the Supplier; and (i) a failure in the Supplier's and/or Authority's supply chain to the extent that such failure is due to any event suffered by a member of such supply chain, which would also qualify as a Force Majeure Event in accordance with this definition had it been suffered by one of the Parties; but excluding, for the avoidance of doubt, an epidemic or pandemic;	
	"Law"	means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply. For the avoidance of doubt, this shall include any Laws arising out of or in connection with any withdrawal of the United Kingdom from the European Union;	
	"Purchase Order"	means the Authority's unique number relating to the supply of the Goods and Services;	
	"Receipt"	means the physical or electronic arrival of the invoice at the address specified above in section 'G' (Invoicing) or at any other address given by the Authority to the Supplier for the submission of invoices from time to time;	

This Contract may be executed in any number of counterparts (including by electronic transmission), each of which when executed shall constitute an original but all counterparts together shall constitute one and the same instrument.

Execution of this Contract may be carried out in accordance with the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (SI 2016/696) and the Electronic Communications Act 2000. In the event each Party agrees to sign this Contract by electronic signature (whatever form the electronic signature takes) it is confirmed that this method of signature is as conclusive of each Party's intention to be bound by this Contract as if signed by each Party's manuscript signature. In such situation, this Contract shall be formed on the date on which both Parties have electronically signed the Contract as recorded in the Authority's electronic contract management system.

BY SIGNING AND RETURNING THIS SLA THE SUPPLIER AGREES to enter a legally binding contract with the Authority to provide the Goods and/or Services. The Parties hereby acknowledge and agree that they have read the Schedule 1 – the Call-off Terms and Conditions and by signing below agree to be bound by the terms of this Contract.

The individuals set out below shall execute this Contract, on behalf of the Authority and the Supplier, either using a manuscript signature or an electronic signature. A manuscript signature shall be placed in the execution block below, an electronic signature shall be evidenced in an execution block to be attached as the final page of this Contract:

[redacted]

DSPT Audit Requirements and Outcomes 23-24

Strategy, objectives, and outcomes

The DSPT Audit It is mandated via the NHS Standard Contract and the DSPT requirement that the following NHS organisations (listed below) annually complete a DSPT audit/independent assessment:

- NHS Trusts (Acute, Foundation, Ambulance and Mental Health)
- Integrated Care Boards
- Commissioning Support Units
- DHSC Arm's Length Bodies

NHS England (NHSE) provides a central audit service to underpin and support this requirement with the objective of meeting the following **outcomes**:

- Providing additional central audit capacity for the system, though leveraging this central service provision provided by NHSE and its suppliers.
- Providing outputs from the central audits on theme's to be used for future input into overall areas of risk, development of future DSPT and improvement programmes, projects services and operational delivery activities.
- Strategically from the implementation / policy position at JCU the audits will be used to look at the CAF like returns (from the mandates scope) and get real feedback on how much the current audit regime could be used for a CAF outcomes-based model.
- From the ARAC (Risk and Audit Committee) to have a small volume (circa 20-30)of centrally funded quality audits that are truly independent (from the organisations being audited) that will see if DSPT returns are reflective of the actual security posture of the organisations being audited.

It is proposed that this will be achieved through the meeting the following **objectives:**

- Gain insight and central intelligence regarding data and cyber security risk themes across the health and care system.
- Receive feedback on this year's fixed scope, to ensure appropriate audit scope continues to be achieved in future years.
- Gain intelligence on any organisations of interest, for example those that are non-compliant.
- Signal a continued central interest and involvement in the audit regime to the wider system, including the audit community.
- Drive compliance regarding DSP Toolkit audit requirements by providing examples of what 'good' looks like.
- Encourage future compliance with the organisations subject to audit.
- Continue to gather feedback on the guidance and approach, to understand its effectiveness in driving consistency, encouraging assessors to measure intent as well as output, and improving assurance.
- Perform independent assessments/internal audits on selected NHS Organisations' DSP Toolkit submission, following the central guidance and fixed scope, set by NHS Digital.
- Report back to NHS Englands (and potentially other key stakeholders) on findings and themes.
- Feedback on the 2023-24 audit/assessment guidance and fixed scope

References:

- News (dsptoolkit.nhs.uk)
- Help (dsptoolkit.nhs.uk)

[redacted]

Scope of work and Deliverables:
The scope of the work is as follows:

1) Perform up to 30 independent assessments/internal audits on selected NHS Organisations' DSP Toolkit submissions using 2 suppliers based on circa 5-25 (maximum) per supplier based on the process and methodology below.
2) The assessment must be performed following the DSPT 23-24 audit scope, as provided by NHSE. The audit scope will be published later in the year .It will be 13 DSPT assertions. https://www.dsptoolkit.nhs.uk/Help/Independent-Assessment-Guides
3) An independent assessment/audit report must be completed for each assessment and must be provided to both the Trust it concerns and NHSE. It must adhere to following specification https://www.dsptoolkit.nhs.uk/Help/Independent-Assessment-Guides
4) To provide One overall documented constructive feedback on the 2023-24 Independent Assessment Guidance, approach, and fixed scope: Feedback on any pain points or areas for improvement concerning the guidance and approach. For each issue found they should list its evidence items, what the issue was and how it manifested itself, what the effect and if negative any proposal on a solution.
5) One annual (approximately April 2024) overall thematic report, presented to NHSE and related interested stakeholders (i.e., Joint Cyber Unit) to be submitted at the end of the time period which will include the items detailed in the thematic report section.

Timescales

- The Audit program is expected to commence January 2024 and conclude March 2024.
- Once a audit has been advised, the Supplier shall work with the NHSE DSPT audit team to agree a schedule of activity and within 2 days of the audit request being received to produce a draft SOW.
- Following confirmation to audit, the audit shall be commenced within 10 working days, subject to organisational preparedness and NHSE agreement.

Commissioning: Process and methodology:
The DSPT Audit team will manage the service and the engagement with the suppliers in the delivery of this service and ensure that a standard methodology is followed which is included in https://www.dsptoolkit.nhs.uk/Help/Independent-Assessment-Guides to ensure consistency and transparency of process and outcomes. Coordination of the audits will be in collaboration with both the supplier and the organisation to be audited to ensure an effective outcome – i.e., availability, capacity of suppliers, sites to be audited, required outcomes and any queries to be resolved collaboratively between all parties before any work commences.

The central DSPT audit team in NHSE will work with the suppliers to:

Identify and agree the scope and volume of organisations to be audited using defined criteria based on:

- Min of 5 and a max of 25 organisations per supplier, this will be determined by the DSPT audit team, using the following criteria in agreement with nominated suppliers.
    - The primary ranking supplier (from the ITT outcome) will be provided with the audit schedule from NHSE followed by the

secondary supplier being provided with a alternative schedule. NHSE shall work collaboratively with suppliers to agree on anomalies in the overall delivery of the full schedule. NHSE shall reserve the right to have any final decision on the schedule. Allocation to primary and secondary will be made on the basis of any confliction, availability to deliver / timescales and if appropriate the suitability of the organisation match with the audit firm (i.e. if they have previously audited them and any unique due diligence considerations). Audits will be allocated on a alternate basis to the primary and secondary supplier until each supplier has completed 5 audits then the matching methodology as described above will be used thereafter.

- Capacity and skills required to complete the audit can be seen in Annex A
- Independent audit assurance (i.e. supplier is independent to organisation to be audited)

- The supplier shall ensure there is a central record of request's along with a defined timetable of audits to be delivered, in line with the overall audit timescales for this service. (see above)
- The supplier must advise the central audit team of any delays or issues with delivery of the agreed audits and work with the DSPT central audit team to agree a pragmatic approach to resolve and deliver within the overall service delivery timescales (i.e. Jan 2024– March 2024)
- The supplier shall ensure that the product of a draft audit report is produced within 10 days of each organisation audited, with a final agreed copy within 20 days.
- All testing must be conducted by experienced and suitably qualified (Annex A see skills/ experience section) audit staff, who are familiar with working to de defined audit scope (i.e., DSPT) in addition to knowledge of the DSPT Toolkit and ideally the Cyber Assurance Framework. If on occasion less experienced staff are utilised, they must always be paired with more experienced team members to ensure delivery to the specification.
- Working documentation, findings and reporting data must be stored within the UK and not shared with any other organisations, other than those within scope of this service, including the supplier, NSE and the Organisations in scope of audit. Where data is shared with other NHSE partners, this will be the decision of the DSPT Audit team and a member of the wider Cyber Operations Senior Leadership Team.
- Thematic reports provided by the supplier(s), shall be produced in draft 10 working days (covered in overall cost) after the final audit delivered (in accordance with the agreed audit schedule) for NHSE DSPT audit Team to review and provide feedback within 1 week. Final copy should be produced 1 week after comments received. The thematic report should include key insights on the themese covered under the audit be BCP, training or policies etc, A RAG status against each one of the in scope standards and assertions and a detailed explanation of what was found and any underlying causes backed with imperial data from the audits and wider learning. The report (or separate report) should also include a critique and constructive feedback of the standard and audit guides with suggestions for improvements in light of the move of the DSPT to a CAF based model.

- The supplier will be asked to present the Thematic reports back to the DSPT Central Audit team and other interested parties (as determined by the DSPT central Audit team). A noticed of 1 week will be provided to arrange this.
- The supplier should review documentation shared and make themselves aware of the service and scope, ensuring they have all the information they require to deliver the service.
- The Call-Off Contract is non-exclusive, and the Authority does not commit to awarding any work as part of this Contract.

Annex A Skills / Experience auditors should have teams with the skills experience from one of the columns (columns with one item are mandatory)

DSPT Audit Experience	**Cyber Qualifications (any 2 of the following)**	**Data Protection (any one)**	**Experience in audit / implementation other frameworks (any one)**
Undertaken DSPT audits to the mandated methodology	ISC2 CISSP	BCS Foundation in Data Protection	ISO 27001
	ISACA CISM	BCS Practitioner in Data Protection	NIST 800-53
	ISACA CISA	IAPP CIPP/E / CIPM	NCSC CAF
	ISO 27001 Lead Auditor		
	Any SANS / GIAC		
	BCS Certification in Information Security		
	EC Council Ethical Hacker		

[redacted]

If you feel you have any equivalent experience / qualifications, please provide de

ANNEX B (the Data Protection Protocol)
Table A – Processing, Personal Data and Data Subjects

The table below sets out the agreed description of the Processing being undertaken in connection with the exercise of the Parties' rights and obligations under the Contract. The Supplier shall comply with any further written instructions with respect to Processing given by the Authority and any such further instructions shall be incorporated into this table:

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor of the following Personal Data: It is not expected that Personal Data will be processed, it is possible that the Supplier will have to process personal information in order to provide services under this Contract.
Subject matter of the Processing	The Processing is needed in order to ensure that the Processor can effectively deliver the Contract to provide the proposed DSP Toolkit assessment services to NHS England and NHS Trusts. The nature and extent to which personnel information will need to be processed in order to fulfil this contract is dependent upon the evidence for each assessment and assertion.
Duration of the Processing	Processing will only happen during the dates of the contract.
Nature and purposes of Processing	The Supplier will only process the Personal Data: (a) to the extent necessary to provide DSP Toolkit assessments to the Authority (including for Supplier's reasonable business purposes such as facilitation and support of our business and quality control, updating and enhancing client records, analysis for management purposes and/or statutory returns); (b) in accordance with the Authority's specific instructions (save to the extent the Supplier reasonably consider such instructions infringe Data Protection Legislation, in which case Supplier shall notify the Authority); or (c) as required by any competent authority or applicable law. The Supplier shall not process or transfer Personal Data to any jurisdiction outside the European Economic Area ("EEA") other than to a country deemed to provide an adequate level of protection for Personal Data by an applicable regulator or to the extent permissible by Data Protection Legislation.

Type of Personal Data being Processed	The type of Personal Data Processed could include name, address, staff number and other personnel data held on the systems of NHS Trusts which the Supplier may need to access in order to deliver the DSP Toolkit assessment services under this Contract.
Categories of Data Subjects	The Data Subjects could include Staff (including volunteers, agents, and temporary workers), Authoritys/ clients, suppliers, patients. The Data Subjects includes is dependent upon the specific requirements and evidence provided for review under this Contract.
Plan for return of the data once the Processing is complete unless requirement under union or member state law to preserve that type of data	Data will only be retained by the Supplier for the period of time required to complete the assessment currently until end of contract. The Supplier will delete or return all Personal Data to the Authority upon request on termination or expiry of this Contract, or at the end of the specific contract and destroy all copies of the Personal Data (save to the extent that retention of copies is required by applicable law or professional regulation).
Data Protection Officer	[redacted]

Definitions

The definitions and interpretative provisions at Schedule 4 (Definitions and Interpretations) of the Contract shall also apply to this Protocol. Additionally, in this Protocol the following words shall have the following meanings unless the context requires otherwise:

"Data Loss Event"	means any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach**;**
"**Data Protection Impact Assessment**" and "**DPIA**"	means an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
"**Data Protection Officer**" and **"Data Subject**"	shall have the same meanings as set out in the UK GDPR;
"**Data Subject Access Request"**	means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.
"**Personal Data Breach**"	shall have the same meaning as set out in the UK GDPR;
"**Protective Measures"**	means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it;
"Protocol" or "Data Protection Protocol"	means this Data Protection Protocol;
"**Sub-processor"**	means any third party appointed to Process Personal Data on behalf of the Supplier related to this Contract.

1 DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor. The only Processing that the Supplier is authorised to do is listed in Table A of this Protocol by the Authority and may not be determined by the Supplier.

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

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

1.3.1 a systematic description of the envisaged Processing operations and the purpose of the Processing;

1.3.2 an assessment of the necessity and proportionality of the Processing operations in relation to the Services;

1.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

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

1.4 The Supplier shall, in relation to any Personal Data Processed in connection with its obligations under this Contract:

1.4.1 process that Personal Data only in accordance with Table A of this Protocol, unless the Supplier is required to do otherwise by Law. If it is so required, the Supplier shall promptly notify the Authority before Processing the Personal Data unless prohibited by Law;

1.4.2 ensure that it has in place Protective Measures, which have been reviewed and approved by the Authority as appropriate to protect against a Data Loss Event, which the Authority may reasonably reject (but failure to reject shall not amount to approval by the Authority of the adequacy of the Protective Measures), having taken account of the:

(i) nature of the data to be protected;

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

(iii) state of technological development; and

(iv) cost of implementing any measures;

1.4.3 ensure that :

(i) the Supplier Personnel do not Process Personal Data except in accordance with this Contract (and in particular Table A of this Protocol);

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

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

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

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

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

1.4.4 not transfer Personal Data outside of the EU unless the prior written consent of the Authority has been obtained and the following conditions are fulfilled:

(i) the Authority or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or Article 37 of the Law Enforcement Directive (Directive (EU) 2016/680)) as determined by the Authority;

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

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

(iv) the Supplier complies with any reasonable instructions notified to it in advance by the Authority with respect to the Processing of the Personal Data;

1.4.5 at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority on termination or expiry of the Contract unless the Supplier is required by Law to retain the Personal Data.

1.5 Subject to Clause 1.6 of this Protocol, the Supplier shall notify the Authority immediately if it:

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

1.5.2 receives a request to rectify, block or erase any Personal Data;

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

1.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this Contract;

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

1.5.6 becomes aware of a Data Loss Event.

1.6 The Supplier's obligation to notify under Clause 1.5 of this Protocol shall include the provision of further information to the Authority in phases, as details become available.

1.7 Taking into account the nature of the Processing, the Supplier shall provide the Authority with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 1.5 of this Protocol (and insofar as

possible within the timescales reasonably required by the Authority) including by promptly providing:

1.7.1 the Authority with full details and copies of the complaint, communication or request;

1.7.2 such assistance as is reasonably requested by the Authority to enable the Authority to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

1.7.3 the Authority, at its request, with any Personal Data it holds in relation to a Data Subject;

1.7.4 assistance as requested by the Authority following any Data Loss Event;

1.7.5 assistance as requested by the Authority with respect to any request from the Information Commissioner's Office, or any consultation by the Authority with the Information Commissioner's Office.

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

1.8.1 the Authority determines that the Processing is not occasional;

1.8.2 the Authority determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; and

1.8.3 the Authority determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Supplier shall allow for audits of its Processing activity by the Authority or the Authority's designated auditor.

1.10 Each Party shall designate a Data Protection Officer if required by the Data Protection Legislation.

1.11 Before allowing any Sub-processor to Process any Personal Data related to this Contract, the Supplier must:

1.11.1 notify the Authority in writing of the intended Sub-processor and Processing;

1.11.2 obtain the written consent of the Authority;

1.11.3 enter into a written agreement with the Sub-processor which give effect to the terms set out in this Protocol such that they apply to the Sub-processor; and

1.11.4 provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.

1.12 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

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

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

1.15 The Supplier shall comply with any further instructions with respect to Processing issued by the Authority by written notice. Any such further written instructions shall be deemed to be incorporated into Table A above from the date at which such notice is treated as having been received by the Supplier in accordance with Clause 27.2 of Schedule 2 of the Contract.

1.16 The Supplier shall, at all times during and after the expiry of the Contract, indemnify the Authority and keep the Authority indemnified against all losses, damages, costs or expenses and other liabilities (including legal fees) incurred by, awarded against or agreed to be paid by the Authority arising from any breach of the Supplier's obligations under this Clause 1 (Data Protection) of this Protocol.

1.17 Subject to Clauses 1.13, 1.14, and 1.15 of this Protocol, any change or other variation to this Protocol shall only be binding once it has been agreed in writing and signed by an authorised representative of both Parties.

[redacted]

ANNEX C (Change Control Process)

Contract Amendment Template Letter:

[Address of Supplier]

Ref: [ ]
Date: [ ]
Contract Amendment No: [ ]

CONTRACT FOR: [ ]

CONTRACT NUMBER: [ ]

With reference to the Contract dated [ ], both Parties have in principle agreed to the following variation[s] to the Contract: [ ]

[These/This amendment[s] relate[s] to [ ]

Please confirm in writing by signing and returning one copy of this letter, within 14 working days of the date of signature on behalf of [Supplier Name] that you accept the variation[s] set out herein.

The Contract, including any previous variations, shall remain effective and unaltered except as amended by this letter.

Words and expressions in this letter shall have the meanings given to them in the Contract.

Signed by an authorised signatory for and on behalf of [Authority Name]
Position:
Signature:
Date:

Signed by an authorised signatory for and on behalf of [Supplier Name]
Position:
Signature:
Date:

Annex 1 – Commissioning Process for future services under individual Statements of Work

The Supplier shall provide any additional Services required by the Buyer in accordance with the commissioning process leading to one or more SOWs substantially based on the template set out below to this Call-Off Contract.

Commissioning Process

Where the Buyer wishes to commission further work under this Call-Off Contract, it shall:

1. Detail the requirements for each individual project including milestones and acceptance criteria and a populated data protection table containing complete and accurate details of the Personal Data Processing applicable to the SOW ("**Project Requirements**") substantially in the format of the SOW template set out in Annex 1.2 to this Call-Off Contract.
2. The Buyer's commercial team will communicate Project Requirements in writing to the Supplier whereupon the Supplier shall have five (5) Working Days (or an alternative time period as set out by the Buyer upon communicating the Project Requirements) to respond. All commissioning requests shall be routed through the Buyer's Commercial department/dedicated Commercial Leads.
3. The Supplier shall respond to the Project Requirements (the "**Supplier's Solution**") in the format specified by the Buyer at the point of communicating the Project Requirements.
4. The Parties will use the commissioning process to assess and agree the data processing requirements for each project, determine the data subjects and data classes to be processed by the Supplier, such details to be included in the relevant SOW.
5. The Supplier's Solution shall include details of how the work will be undertaken, a timeline/activity plan along a summary of the resources, it shall also include a detailed price for the delivery of the Project Requirements in the format provided by the Buyer. Where no format is specified a section 3 (above) the method used to calculate the price shall be set out in sufficient detail for the Buyer to understand how the price was determined and, as a minimum, the Supplier's pricing will be broken down by the day rates of resources proposed to fulfil the Supplier's Solution and will be no more expensive than the day rates set out in its tender.
6. Fixed fee pricing will be used.
7. Within five (5) Working Days of receipt of the Supplier's Solution, or in any other time period the Buyer deems appropriate, it shall review and feedback comments on the Supplier's Solution.
8. Within two (2) Working Days of the Buyer providing this feedback (or an alternative time period as set out by the Buyer upon communicating its feedback) the Supplier shall provide a final Supplier's Solution to the Buyer.
9. Where the Buyer agrees with either the initial or revised Supplier's Solution the Supplier's Solution shall be attached to the proposed SOW containing the Project Requirements and the Buyer shall sign and return the proposed SOW to the Supplier for countersigning whereupon the Supplier shall commence delivery of the Services detailed in the SOW.
10. Amendments to the SOW (and associated pricing) after the execution of the associated SOW shall follow the variation process set out at clause 24 of the Core Terms and actioned through the Commercial Team.

11. At any point during or before the Commissioning Process, the Buyer may seek alternative means of delivering the requirement including potentially re-competing the requirement.
12. The Call-Off Contract is non-exclusive, and the Buyer does not commit to awarding any additional work as part of this Call-Off Contract.
13. Each SOW will have a unique identifying number supplied by the Buyer.

Security requirements

Some projects may require Supplier's resources to be cleared to the Buyer's security clearance level of Security Check (SC). Some projects may require a higher or lower level of clearance. The level of security clearance required will be communicated in the Project Requirements and prior to each SOW commencing. The Buyer will make best endeavours in providing as much prior notice as is possible in such an event.

1.2 SOW Template

[redacted]

Upon agreement, this SOW will form part of the Call-Off Contract referenced below.

The Parties will execute a SOW for each of the Buyer requirements. Any ad-hoc Service requirements are to be treated as individual requirements in their own right; and the Parties should execute a separate SOW in respect of each, or alternatively agree a variation to the existing SOW via a change control notice (CCN).

The rights, obligations and details agreed by the Parties and set out in this SOW apply only in relation to the Services that are to be delivered under this SOW and will not apply to any other SOWs executed or to be executed under this Call-Off Contract unless otherwise agreed by the Parties.

Unless otherwise explicitly specified in this SOW, the terms of the Call-Off Contract shall apply to the scope of work set out in this SOW unamended. Unless otherwise specified, changes made to the terms of this Call-Off Contract set out herein only apply to the scope of work as set out in this SOW.

The Parties agree that upon signature by both parties, this SOW is a valid variation of the Call-Off Contract under the Order From and clause 24 (Changing the contract) of the Core Terms, and this SOW forms part of the Call-Off Contract as referenced below.

Date of SOW:	
SOW Title:	
SOW Contract Reference:	
Call-Off Project Reference:	
Atamis Contract Reference:	
Workplan:	
Buyer Portfolio Number:	
Buyer:	Health and Social Care Information Centre (known as NHS Digital)
Supplier:	
Commencement Date:	
Completion Date:	
Duration of SOW	
Charging Method(s) for this SOW:	
Key Buyer Staff	
Key Supplier Staff	
Subcontractors	

[redacted]

2. PROGRAMME CONTEXT	
Programme Background	
Delivery Phase	Choose an item.
Overview of Requirement	

3. BUYER REQUIREMENTS	
Deliverables	
Delivery Plan	
Dependencies	
Supplier Resource Plan	
Additional Requirements	

4. CHARGES

The applicable charging method(s) for this SOW is (check one):

Capped Time and Materials	☐	Fixed Price	☐	Incremental Fixed Price	☐

The estimated maximum value of this SOW is: £[ ]

The Charges detailed in the financial model shall be invoiced in accordance with the process outlined in the Order Form.

Financial Model	

5. SECURITY REQUIREMENTS

The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables, have completed Supplier Staff Vetting.

6. LOCATION

The Services outlined within this SOW will be delivered to:
Primary Location:

If not exclusively at the Primary Location, please provide approximate split across other locations. This will be used to calculate blended rates:

Leeds	London	Home / Virtual	Loc 1	Loc 2	Loc 3

%	%	%	%	%	%

Offshore roles are permitted under this Statement of Work	☐

[Buyer Guidance: Please provide a brief explanation of any location split e.g. the work will be based out of Leeds, on average individuals will have to spend approximately one day a week in the Leeds office, the rest of the time they can work either virtually or from their home office.]

7. CHANGE PROCESS

In the event of a change being required to this Statement of Work, the Parties will follow clause 24 (Changing the contract) of the Core Terms.

8. TERMINATION WITHOUT CAUSE

The Buyer shall have the right to terminate this Statement of Work at any time by issuing a Termination Notice to the Supplier giving at least (10) days written. [or other timescale the parties agree per SOW]

9. PROCESSING OF PERSONAL DATA

Unless explicitly noted below, this SOW shall be covered by the arrangements contained in Joint Schedule 11 (Processing Data).

This Statement of Work requires specific Data Processing arrangements	☐

Where the data protection table at Joint Schedule 11 (Processing Data) does not accurately

reflect the Processor / Controller arrangements applicable to this Statement of Work, the parties shall complete the table below with the SOW specific data processing arrangements, in replacement of the table incorporated in Joint Schedule 11 (Processing Data).

Description	Details
Identity of the Controller and Processor	
Subject matter of the Processing	
Duration of the Processing	
Nature and purposes of the Processing	
Type of Personal Data	
Categories of Data Subject	
Plan for return and destruction of the data once the Processing is complete	
Sub-processors	
Data Protection Officers	Buyer's DPO : [tbc] Supplier's DPO : [tbc]

10. INTELLECTUAL PROPERTY RIGHTS

As per clause 9 (Intellectual Property Rights) of the Core Terms, save as expressly granted elsewhere under this Call-Off Contract, the Supplier shall not acquire any right, title, or interest in or to the Intellectual Property Rights of the Buyer.

Unless specifically noted below the Supplier agrees that the Deliverables under this Statement of Work will not, in any way, be dependent on either Supplier or Supplier furnished 3rd Party IPR

One or more Deliverables under this Statement of Work will be dependent of Supplier and/or Supplier furnished 3rd Party IPR as detailed below	☐
The specific IPR (and associated licence terms) are detailed in:	[Buyer Guidance: applicable licence terms should be attached as an Appendix to this Statement of Work]

11. IR35 DETERMINATION STATEMENT

IR35 Status Determination Statement	
Required	[ ]
Not Required	[ ]

12. SIGNATURES AND APPROVALS

Agreement of this SOW

BY SIGNING this Statement of Work, the parties agree that it shall be incorporated into the Order Form and the Call-Off Contract

and be legally binding the Parties:

For and on behalf of the Supplier	Name and title	
	Date	

	Signature	
For and on behalf of the Buyer	Name and title	
	Date	
	Signature	