Crown Commercial Service

Technology Products 2 Agreement RM3733
Framework Schedule 4 - Annex 1

Order Form

In this Order Form, capitalised expressions shall have the meanings set out in Call Off Schedule 1 (Definitions), Framework Schedule 1 or the relevant Call Off Schedule in which that capitalised expression appears.

The Supplier shall supply the Goods and/or Services specified in this Order Form to the Customer on and subject to the terms of the Call Off Contract for the duration of the Call Off Period.

This Order Form should be used by Customers post running a Further Competition Procedure under the Technology Products 2 Framework Agreement ref. RM3733.

The Call Off Terms, referred to throughout this document, are available from the Crown Commercial Service website at http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3733

Crown Commercial Service

Section A
General information

This Order Form is issued in accordance with the provisions of the Technology Products 2 Framework Agreement RM3733.

Customer details	
Customer organisation name **Element 1:** Department for Health and Social Care ("DHSC") **Element 2:** NHS Digital	
Billing address Your organisation's billing address - please ensure you include a postcode	
Element 1: DHSC REDACTED TEXT REDACTED TEXT REDACTED TEXT	**Element 2:** NHS Shared Business Services REDACTED TEXT REDACTED TEXT REDACTED TEXT REDACTED TEXT REDACTED TEXT
Customer representative name The name of your point of contact for this Order	
Element 1: REDACTED TEXT	**Element 2:** REDACTED TEXT
Customer representative contact details Email and telephone contact details for the Customer's representative	
Element 1: REDACTED TEXT REDACTED TEXT	**Element 2:** REDACTED TEXT REDACTED TEXT

Supplier details
Supplier name The Supplier organisation name, as it appears in the Framework Agreement

Crown Commercial Service

Bytes Software Services Ltd

Supplier address
Supplier's registered address
Bytes House, Randalls Way, Leatherhead, Surrey, KT22 7TW

Supplier representative name
The name of the Supplier point of contact for this Order
REDACTED TEXT

Supplier representative contact details
Email and telephone contact details of the supplier's representative
REDACTED TEXT

Order reference number
REDACTED TEXT

Crown Commercial Service

Section B
Overview of the requirement

Framework Lot under which this Order is being placed
Tick one box below as applicable

1.	HARDWARE	☐
2.	SOFTWARE	☒
3.	COMBINED SOFTWARE AND HARDWARE REQUIREMENTS	☐
4.	INFORMATION ASSURED PRODUCTS	☐
5.	VOLUME HARDWARE REQUIREMENTS (DIRECT FROM OEM)	☐

Customer project reference
Please provide a project reference, this will be used in management information provided by suppliers to assist CCS with framework management
CCSO18A15 – Microsoft Windows 10 ESA for NHS

Call Off Commencement Date
The Call Off Commencement Date is the date on which the Call Off Contract is formed – this should be the date of the last signature on Section E of this Order Form
30/04/2018

Call Off Contract Period (Term)
A period in Months which does not exceed 60 Months (5 years) - **leave blank if this is a simple transactional Goods purchase**. Where established as an initial and extension period complete the fields below

Element 1: 60 months

Element 2: 36 months commencing 25th May 2018

Call Off Initial Period Months
N/A

Call Off Extension Period (Optional) Months
N/A

Specific Standards or compliance requirements
Include any conformance or compliance requirements with which the Goods and/or Services must meet
Click here to enter text.
The Parties agree to the inclusion of the following clauses relating to compliance requirements:

1. **Corporate Social Responsibility Conduct and Compliance**

1.1 The Customer applies corporate and social responsibility values to its business operations and activities which are consistent with the Government's corporate social responsibility policies, including, without limitation, those policies relating to anti-bribery and corruption, health and safety, the environment and sustainable development, equality and diversity.

1.2 The Supplier represents and warrants that it:

1.2.1 complies with all CSR Laws;

1.2.2 requires its Sub-Contractors and any person under its control, to comply with all CSR Laws; and

1.2.3 has adopted a written corporate and social responsibility policy that sets out its values for relevant activity and behaviour (including, without limitation, addressing the impact on employees, clients, stakeholders, communities and the environment by the Supplier's business activities).

1.3 The Supplier shall notify the Customer in the event that its 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.

2. Modern Slavery

2.1 The Supplier represents and warrants that at the Call Off Commencement Date neither the Supplier, nor any of its officers and employees:

2.1.1 have been convicted of any offence involving slavery and human trafficking; and

2.1.2 having made reasonable enquiries, so far as it is aware, have been or is the subject of any investigation, inquiry or enforcement proceedings by any governmental, administrative or regulatory body regarding any offence or alleged offence of or in connection with slavery and human trafficking.

2.2 The Supplier shall implement due diligence procedures for its Sub-Contractors and other participants in its supply chains to ensure that there is no slavery or human trafficking in its supply chains.

2.3 The Supplier shall prepare and deliver to the Customer each year, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business.

3. Data Protection

Crown Commercial Service

3.1 The following provisions in relation to the Processing of Personal Data shall replace Clause 15.7 (Protection of Personal Data) of the Call Off Contract.

3.2 Where any Personal Data are Processed in connection with the exercise of the Parties' rights and obligations under the Call Off Contract, the Parties acknowledge that the Supplier shall be acting as a Processor on behalf of the Authority as the Controller. The only Processing that the Supplier is authorised to do is listed in Clause 3.14 and may not be determined by the Supplier.

3.3 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 Customer, include:

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

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

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

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

3.4 The Supplier shall, and shall procure that its agents, Sub-Processors and employees shall:

3.4.1 Process the Personal Data only in accordance with instructions from the Authority (which may be specific instructions or instructions of a general nature as set out in the Call Off Contract, or as otherwise notified by the Authority to the Supplier in writing from time to time) and Clause 3.14, 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;

3.4.2 notify the Customer immediately if it considers that any of the Authority's instructions infringe the Data Protection Laws;

3.4.3 ensure that at all times it has in place appropriate technical and organisational measures (which are consistent with Article 32 of the GDPR) to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction, or damage to the Personal Data, such measures to ensure a level of security commensurate with the risks associated with the Processing, and including the measures set out in this Clause 3, having taken account of the:

(a) nature of the data to be protected;
(b) harm that might result from a Personal Data Breach;

(c) state of technological development; and
(d) cost of implementing any measures;

3.4.4 notify the Authority immediately upon becoming aware of a Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the Authority with sufficient information to meet any obligations to report a Personal Data Breach under the Data Protection Laws. Such notification shall as a minimum:

(a) describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
(b) communicate the name and contact details of the data protection officer or other relevant contact from whom more information may be obtained;
(c) describe the likely consequences of the Personal Data Breach; and
(d) describe the measures taken or proposed to be taken to address the Personal Data Breach;

3.4.5 co-operate with the Customer and take such reasonable steps as are directed by the Customer to assist in the investigation, mitigation and remediation of a Personal Data Breach;

3.4.6 not disclose the Personal Data to any Supplier staff unless necessary for the provision of the Services;

3.4.7 other than where specifically authorised under the Call Off Contract, not appoint any third party sub-contractor to Process the Personal Data (**"Sub-Processor"**) without the prior written consent of the Customer. In all cases where a Sub-Processor is appointed:

(a) the contract between the Supplier and the Sub-Processor shall include terms which are substantially the same as those set out in this Clause 3;
(b) the Supplier shall provide the Authority with such information regarding the Sub-Processor as the Authority may reasonably require;
(c) the Supplier shall remain fully liable to the Authority for any failure by a Sub-Processor to fulfil its obligations in relation to the Processing of any Personal Data; and
(d) the use of the Sub-Processor shall be otherwise in accordance with Clause 3.5;

3.4.8 take reasonable steps to ensure the reliability and integrity of any Supplier staff who have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Personal Data, as strictly necessary to perform the Services in the context of that individual's duties to the Supplier, and ensure that the Supplier staff:

(a) are aware of and comply with the Supplier's obligations under this Clause 3 together with any obligations pertaining to confidentiality or data protection which are set out in the Call Off Contract;
(b) are subject to confidentiality undertakings or other contractual or professional or statutory obligations of confidentiality;
(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 Customer or as otherwise permitted by the Call Off Contract; and
(d) have undergone adequate training in the use, care, protection and handling of Personal Data;

3.4.9 notify the Authority immediately if it receives:

(a) from a Data Subject (or third party on their behalf):

(i) a Data Subject Access Request (or purported Data Subject Access Request);
(ii) a request to rectify any inaccurate Personal Data;
(iii) a request to have any Personal Data erased or blocked;
(iv) a request to restrict the Processing of any Personal Data;
(v) a request to obtain a portable copy of Personal Data, or to transfer such a copy to any Third Party; or
(vi) an objection to any Processing of Personal Data;

(b) any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data under the Call Off Contract;

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

(each a **"Relevant Communication"**).

3.4.10 taking into account the nature of the Processing, provide the Authority with full cooperation and assistance (within the timescales reasonably required by the Authority, and in any case within sufficient time for the Customer to comply with any relevant timescales prescribed by the Data Protection Laws) in relation to any Relevant Communications (whether received by the Supplier or by the Customer directly) including by implementing such technical and organisational measures as may be reasonably required by the Authority and by promptly providing:

(a) the Customer with full details and copies of the Relevant Communication (where received by the Supplier);
(b) the Customer, on request by the Customer, with any Personal Data it holds in relation to a Data Subject; and
(c) assistance as requested by the Customer with respect to any request from the Information Commissioner's Office, or any consultation by the Customer with the Information Commissioner's Office;

3.4.11 allow for audits (including inspections) of its data Processing activity by the Customer or the Customer's mandated Auditor, and if requested by the Customer, provide a written description of the measures that it has taken and technical and organisational security measures in place, for the purpose of compliance with its obligations pursuant to this Clause 3 and provide to the Customer copies of all documentation relevant to such compliance including, protocols, procedures, guidance, training and manuals.

3.4.12 cease Processing the Personal Data immediately upon the earlier of the (i) termination or expiry of the Call Off Contract, or (ii) the cessation of the Services, and as soon as reasonably practicable thereafter, at the Customer's option, either return, or securely and irrevocably delete from its systems (so that such Personal Data cannot be recovered or reconstructed), the Personal Data and any copies of it or of the information it contains; and

3.4.13 designate a data protection officer if required by the Data Protection Laws.

3.5 The Supplier shall not Process or otherwise transfer, or permit the transfer, of any Personal Data in or to any Restricted Country without obtaining the prior written consent of the Customer (unless the transfer is required by EU or member state law to which the Supplier is subject, and if this is the case then the Supplier shall inform the Customer of that requirement before Processing the Personal Data, unless a Law prohibits such being provided on important grounds of public interest).

3.6 In respect of any Processing in, or transfer of Personal Data to, any Restricted Country permitted in accordance with Clause 3.5, the Supplier shall, when requested by the Customer, promptly enter into an agreement with the Customer or any service recipient including or on such provisions as the Standard Contractual Clauses and/or such variation as a regulator or the Customer might require which terms shall, in the event of any conflict, take precedence over those in this Clause 3, and the Supplier shall comply with any reasonable instructions notified to it in advance by the Authority with respect to the transfer of the Personal Data;

3.7 Subject to the Authority providing the Supplier with all information reasonably required by the Supplier to comply with this Clause 3.7, create and maintain a register setting out:

3.7.1 the types of Personal Data and categories of Data Subject whose Personal Data are Processed during the provision of the Services; and information

3.7.2 a general description of the technical and organisational security measures adopted by the Supplier to protect the Personal Data in accordance with Clause 3.4..3.

3.8 The Supplier shall use its reasonable endeavours to assist the Authority to comply with any obligations under the Data Protection Laws and shall not perform its obligations under the Call Off Contract in such a way as to cause the Authority to breach any of the Authority's obligations under the Data Protection Laws to the extent the Supplier is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

3.9 Both the Authority and the Supplier shall comply with their respective obligations under the GDPR in relation to the Call Off Contract, including by adhering to any relevant codes of conduct published pursuant to Article 40 of the GDPR.

3.10 Both the Authority and the Supplier shall comply with their respective obligations under any relevant law implementing or otherwise giving effect to the NIS Directive. In response to the obligations created by any law implementing or otherwise giving effect to the NIS Directive, the Authority may elect to produce a report setting out the steps to be reasonably followed by both parties in relation to their compliance with the NIS Directive in the context of the Services, and the Supplier shall comply with the terms of any such report.

3.11 Notwithstanding any other provision in the Call Off Contract relating to amendments or variations to the Call Off Contract, the Authority may, at anytime on not less than 30 Working Days' notice, revise this Clause 3 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 the Call Off Contract).

3.12 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Authority may on not less than 30 Working Days' notice to the Supplier amend the Call Off Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

3.13 If following the date of the Call Off Contract:

3.13.1 any codes of practice, codes of conduct, regulatory guidance, standard clauses and any other related laws arising from the GDPR or from the NIS Directive are published; or

3.13.2 the UK ceases to be a Member State of the European Union, then the Authority may require the Supplier to take such further reasonable actions, or enter into

such further contractual terms, in each case as necessary to take account of these developments.

3.14 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 Call Off 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:

[Please note that this table has been completed with information pertaining to Element 1 ONLY. The table will be finalized following completion of the Call Off Contract for Element 2]

Description	Details
Subject matter of the Processing	Bytes are assisting NHS Digital in management of Microsoft Windows Licence Allocations to Local NHS Organisations. To do this they need to record NHS staff information for the purpose of maintaining contact with them throughout the agreement. Also to keep records of signatures (physical and electronic) by senior staff agreeing to the terms of the NHS Digital Service Agreement on behalf of their organisations in order to receive the licences.
Duration of the Processing	*30th April 2018 to 30th April 2023 inclusive*
Nature and purposes of Processing	*NHS Informatics Staff with interests in use of the Microsoft Windows Licensing from either an ICT operational or cybersecurity protection standpoint will be recorded and maintained by Bytes to allow them to effectively communicate with NHS local organisations on behalf of NHS Digital.* *Bytes will also maintain records of signed NHS Digital Service Agreements (and details of signatories) which must be signed by local organisations in return for provision of free licensing by NHS Digital.*
Type of Personal Data	*NHS staff names, job titles, email, phone, mobile contact details, linked to the NHS organization they work for and the ODS code for that organization.*
Categories of Data Subjects	*NHS Staff, permanent and temporary who are responsible for managing the ICT estate of local*

	organisations and are thus involved in the deployment and operation of the licences administered by Bytes.
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	*The information will be captured and maintained throughout the course of Bytes agreement (April 30th 2018 to April 30th 2023). A copy of the records at the then current state will be provided to NHS Digital at the end of the agreement.*

3.15 The Controller could be the Authority and/or other parties and therefore all references to the Authority in this Clause 3.15 shall be interpreted to extend to any other Controller as if they were a party to the Call Off Contract.

4. Cyber Security Requirements

The Supplier warrants and represents that it has complied with and throughout the Call Off Contract Period will continue to comply with the Cyber Security Requirements.

5. Grant of licences by the Supplier

Notwithstanding any other clause in the Call Off Contract, the Parties agree that any licence granted pursuant to clause 14.2 (*Licences granted by the Supplier: Specially Written Software and Project Specific IPR*) shall be done so on terms no less favourable to the Customer than those set out by clause 14.2 (*Licences granted by the Supplier: Specially Written Software and Project Specific IPR*) of the template Call Off Contract attached to the Framework Agreement, unless expressly agreed otherwise by the Customer.

6. Approval of Key Sub-Contractors

6.1 Where the Supplier wishes to enter into a new Key Sub-Contract or replace a Key Sub-Contractor, it must obtain the prior written consent of the Authority and the Customer (the decision to consent not to be unreasonably withheld or delayed). The Authority and/or the Customer may reasonably withhold its consent to the appointment of a Key Sub-Contractor if any of them considers that:

(a) the appointment of a proposed Key Sub-Contractor may prejudice the provision of the Services or may be contrary to its interests;

(b) the proposed Key Sub-Contractor is unreliable and/or has not provided reasonable services to its other customers; and/or

(c) the proposed Key Sub-Contractor employs unfit persons.

6.2 Except where the Authority and the Customer have given their prior written consent under Clause 7.1 (Approval of Key-Sub-Contractors), the Supplier shall ensure that each Key Sub-Contract shall include:

(a) a right under CRTPA for the Customer to enforce any provisions under the Key Sub-Contract which confer a benefit upon the Customer;
(b) a provision enabling the Customer to enforce the Key Sub-Contract as if it were the Supplier; and
(c) obligations no less onerous on the Key Sub-Contractor than those imposed on the Supplier under the Call Off Contract.

7. Execution and Counterparts

This Call Off Contract may be executed in counterparts, each of which when executed shall constitute an original but all counterparts together shall constitute one and the same instrument. Execution of this Call Off Contract may be carried out in accordance with EU Directive 99/93 (Community framework for electronic signatures) and the Electronic Communications Act 2000, and in such situation, this Call Off Contract shall be formed on the date on which both Parties have communicated acceptance of its terms.

8. Cyber Security Requirements

The Cyber Security Requirements set out in Appendix 1 to this Order Form shall be added as a new Schedule 5 (Cyber Security Requirements) of the Call Off Contract.

9. Definitions

Within the scope of the Call-Off Contract, the following definitions shall be added to Schedule 1 - Definitions:

"Competent Authority" means the public authority(ies) or similar regulatory authority(ies) designated as being competent by the UK Government to be responsible for the implementation of the NIS Directive and ensuring compliance with its provisions;

"Controller" or **"Data Controller"** has the meaning given to it in the Data Protection Laws;

"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;

Crown Commercial Service

“CSR Policies” means the Customer’s policies, including, without limitation, anti-bribery and corruption, health and safety, the environmental and sustainable development, equality and diversity, and any similar policy notified to the Supplier by the Customer from time to time, and “**CSR Policy**” shall mean any one of them;

"Customer Personal Data" means the Personal Data supplied by the Customer to the Supplier for purposes of, or in connection with, the Call Off Contract;

“Cyber Security Requirements” means:

a) compliance with the IG Toolkit or any replacement of the same;

b) the Cyber Security Requirements in Schedule 5 of the Call Off Contract; and
c) any other cyber security requirements relating to the Services notified to the Supplier by the Customer from time to time;

"Data Protection Impact Assessment" means an assessment by the Customer of the impact of the envisaged processing on the protection of Personal Data;

"Data Protection Laws" 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, until 25 May 2018, the Data Protection Act 1998 and from 25 May 2018, Regulation (EU)_2016/679, 'the General Data Protection Regulation' (**"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;

"Data Subject" has the meaning given to it in the Data Protection Laws;

"Data Subject Access Request" means a request made by a Data Subject in accordance with rights granted pursuant to the Data Protection Laws to access his or her Personal Data;

"**IG Toolkit**" means the Department of Health's information governance toolkit, which includes the policies and standards required by the Department of Health, and which can be accessed from https://www.igt.hscic.gov.uk/, as may be amended by the Customer or the Department of Health from time to time;

"NIS Directive" means the Network and Information Security Directive (EU/2016/1148) and all implementing legislation passed by the UK Government and guidelines, guidance notes, codes of practice and codes of conduct issued from time to time by a Competent Authority;

Crown Commercial Service

"Personal Data" has the meaning given to it in the Data Protection Laws, and applies to personal data which is Processed by the Supplier or any Sub-Contractor on behalf of the Customer or a Central Government Body pursuant to or in connection with the Call Off Contract;

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;

"Process" has the meaning given to it in the Data Protection Laws, and **"Processed"** and **"Processing"** shall be construed accordingly;

"Reportable Incident" shall have the meaning given to it in the NIS Directive;

"Restricted Country" means any country which is not (i) a member of the European Economic Area; (ii) the United Kingdom; (iii) deemed adequate by the European Commission pursuant to article 25(6) of Directive 95/46/EC or article 45(3) of the General Data Protection Regulation;

"Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection as set out in Commission Decision C (2010) 593 and reference to the standard contractual clauses shall be to the clauses as updated, amended, replaced or superseded from time to time by the European Commission; and

"Sub-Processor" has the meaning given to it in Clause 3.4.7.

Crown Commercial Service

Section C
Customer Core Goods and/or Services Requirements

Please provide details of all Goods and/or Services required (including any items which are considered business critical) including the locations where the supplier will be required to deliver the service/s Ordered**.**

Goods and/or Services

The goods and services to be provided within this contract are outlined in **Annex 4a – Appendix B – Statement of Requirements.**
Annex 4b – Clarification Reponses provides further clarification around Annex 4a that was requested and confirmed as part of the tender submissions for this contract.

In addition to these documents, **Annex 5a through to Annex 5e – Bytes Tender Submission** further sets out the goods and services to be delivered by the Supplier to the Customer for the purpose of this contract.

The key features of all documents can be outlined as followed:

Element 1 - Microsoft Windows 10 ESA

The provision of two (2) types of MS10 Licences, as follows:

SKU	Product	Volume
AAA-22363	Windows E5 Per Device Subs VL	965,170
AAA-51072	Windows VDA E5 Per Device Subs	34,830

Any additional MS10 Licences that are required by the Authority will be purchased and managed at the same unit price over the term of the ESA.

The Authority further requires the following management services for the MS10 Licences for the term of the ESA:

- Reporting and Recording
- Deployment of new MS10 Licences
- Management of existing MS10 Licences
- Management of MS10 Licences during the term

Element 2 – Microsoft LSP for NHS Digital:

Crown Commercial Service

NHS Digital requires the renewal of its Microsoft estate licences, Azure Hosting and Premier Support for a three (3) year period, commencing on 25th May 2018.

This list outlined in Annex 4 – Appendix B – Statement of Requirement is an indication of the products to be purchased only. Any changes to this list will be communicated to the Supplier prior to 25th May 2018 and will be subject to the change procedure of the Contract.

The Supplier will work alongside the Authority to understand the Authority's Microsoft licence requirements and advise on the appropriate software licences and quantities based on its knowledge of Microsoft products.

The Supplier will present options of licencing structures which will enable the Authority optimise licencing and cost benefits to support annual renewals and new purchasing requirements throughout the three (3) year term of the LSP Agreement

The Supplier will also be responsible for notifying the Authority in a timely advanced manner of any commitment dates/deadlines associated with the available licence structures to ensure the Authority is able to take full advantage of any opportunities available.

The Supplier will handle paperwork with Microsoft for annual commitments and ad-hoc orders.

The Supplier will help obtain licences and ensure these are allocated to the correct enrolment. The next anniversary date for Element 2 commitment is 25th May 2018.

Warranty Period, if applicable
In line with Microsoft Warranty and the standard Warranty for Goods as laid out in Annex 2 – Terms and Conditions

Location/Site(s) for Delivery

Element 1:
REDACTED TEXT
REDACTED TEXT

Dates for Delivery of the Goods and/or the Services

Element 1: 27/04/2018

Element 2: 25/05/2018

Software List product details under each relevant heading below

Crown Commercial Service

Supplier Software	Third Party Software	Maintenance Agreement
N/A	In line with NHS Microsoft 10 Windows Enterprise Agreement (reference to be advised following contract completion) Include license or link in Call Off Schedule 3	In line with NHS Microsoft 10 Windows Enterprise Agreement (reference to be advised following contract completion) Include terms or link in Call Off Schedule 3

Additional Clauses (see Annex 3 of Framework Schedule 4) Tick as required

Alternative Clauses		Additional Clauses Tick one box below as applicable		Optional Clauses Tick any applicable boxes below	
Scots Law Or	☐	A: Termed Delivery – Goods	☒	C: Due Diligence	☐
Northern Ireland Law	☐	B: Complex Delivery – Solutions (includes Termed Delivery – Goods)	☐	D: Call Off Guarantee	☐
Non-Crown Bodies	☐	**NB Both of the above options require an Implementation Plan which should be appended to this Order Form**		E: NHS Coding Requirements	☐
Non-FOIA Public Bodies	☐			F: Continuous Improvement & Benchmarking	☐
				G: Customer Premises	☐
				H: Customer Property	☐
				I: MOD Additional Clauses	☐

Items licensed by the Customer to the Supplier (including any Customer Software, Customer Background IPR and Customer Data)
List below
N/A

Call Off Contract Charges payable by the Customer to the Supplier (including any applicable Milestone Payments and/or discount(s), but excluding VAT) and payment terms/profile including method of payment (e.g. Government Procurement Card (GPC) or BACS)
See Annex 6 – Call Off Contract Charges.
Please note that for the purpose of Element 2, the Margin listed in Annex 6 will be applied against the Reseller Buy Price for all licences purchased under this element of the requirement.

Is a Financed Purchase Agreement being used? Tick as required	☐ If so, append to Call Off Schedule 2 as Annex A
Estimated Year 1 Call Off Contract Charges (£) For Orders with a defined Call Off Contract Period	£29,241,017.57

Section D
Supplier response

Suppliers - use this section to provide any details that may be relevant in the fulfilment of the Customer Order

Commercially Sensitive information
Any information that the Supplier considers sensitive for the duration of an awarded Call Off Contract
none

Total contract value
Please provide the total contract value (for the Call Off Initial Period) as detailed in your response to the Customer's statement of requirements

Please see Annex 6 – Call Off Contract Charges

Crown Commercial Service

Section E
Call Off Contract award

This Call Off Contract is awarded in accordance with the provisions of the Technology Products 2 Framework Agreement RM3733.

The Supplier shall supply the Goods and/or Services specified in this Order Form to the Customer on and subject to the terms of this Order Form and the Call Off Terms (together referred to as "the Call Off Contract") for the duration of the Call Off Contract Period.

SIGNATURES

For and on behalf of the Supplier

Name	REDACTED TEXT
Job role/title	**Director of Public Sector**
Signature	REDACTED TEXT
Date	**27/04/2018**

For and on behalf of the Customer

Name	REDACTED TEXT
Job role/title	**Deputy Director**
Signature	REDACTED TEXT
Date	**27/04/2018**

Crown Commercial Service

Appendix 1

CALL OFF SCHEDULE 5: CYBER SECURITY REQUIREMENTS

In this Schedule:

"Access Control Lists (ACL)"	shall mean with respect to a computer file system, a list of permissions (such as users, system processes) which are attached to (or permitted to be granted to) an object;
"Approved Cryptographic Algorithms Good Practice Guideline"	shall mean the Approved Cryptographic Algorithms Good Practice Guideline set out in Appendix 1 or any replacement of the same as notified to the Supplier by the Authority;
"Authority Information"	shall mean all information, including Confidential Information, data, Intellectual Property Rights and Personal Data, however it is conveyed or received, that (without prejudice to the foregoing) relates to the customers, business affairs, development, trade secrets, business plans, know-how, personnel or suppliers of the Authority or any Authority Service Recipients together with any information derived from any of the above;
"Authority Records"	shall mean any record of Authority Information in any format or media which provides evidence of business activity;
"Authority Security and Cyber Policies and Rules"	shall mean all policies, standards and rules encompassed within the policy framework owned by the Authority;
"Authority System"	shall mean the Authority's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Authority or the Supplier in connection with this Agreement which is owned by the Authority or licensed to it by a third party;
"Border Gateway Protocol"	shall mean a standardised exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet;

"CREST"	shall mean CESG Registered Ethical Security Tester;
"Cyber Attack"	shall mean any unauthorised attempt to gain unauthorised control, disrupt or cause a denial of service in relation to the Authority Information and / or the Authority System;
"DDoS Attack"	shall mean a distributed and non distributed denial of service attempt or attempts to make an online service unavailable by overwhelming it with Traffic or connections from multiple sources;
"Good Industry Practice"	shall mean in relation to any undertaking and any circumstances and in particular the provision of services to UK Government bodies or organisation of similar standing, the exercise of that degree of professionalism, skill, diligence, prudence, care, efficiency, timeliness, judgement and foresight which would reasonably and ordinarily be expected from a leading and expert internationally recognised company engaged in the same type of activity under the same or similar circumstance seeking to comply with its contractual obligations in full and complying with applicable Laws;
"IT Disaster Recovery and Business Continuity Policy"	shall mean the Authority's policy relating to IT disaster recovery and business continuity in place from time to time;
"Malicious Traffic"	shall mean Traffic, including any unauthorised communication data that contains Malware which is being or is likely to be being transmitted solely for the purposes of a Cyber Attack;
"Malware"	shall mean any software, computer program, code or programming instructions intentionally constructed with the ability to damage, adversely alter, adversely interfere with or otherwise adversely affect, computer programs, data files, equipment, software or operation of computer systems, including Authority System or Supplier System or any other computer program code typically designated to be a ‘virus’, ‘worm’, ‘trojan,’ ‘time or logic bomb’, ‘disabling code’, ‘authorisation key’, ‘licence control utility’ or

	'software lock' or 'routine key-logger', 'sniffer', 'backdoor' or similar;
"Records Policy"	shall mean as defined in paragraph 9.7;
"Recovery Point Objective" or "RPO"	shall mean the acceptable amount of data loss measured in time following the failure of a system;
"Recovery Time Objective" or "RTO"	shall mean the time required to switch from the primary system to a disaster recovery system from the point of recovery invocation;
"Required DDoS Filtering Capacity"	shall mean 150% of the capacity required to prevent the largest DDoS Attack at any time publicly reported or known;
"Retained Data"	shall mean as defined in paragraph 13.6.1;
"Security and Cyber Incident"	shall mean as defined in paragraph 6.1.7;
"Security and Cyber Incident Management Procedures"	shall mean as defined in paragraph 6.1;
"Security and Cyber Policy"	shall mean as defined in paragraph 2.1;
"Security Audits"	shall mean as defined in paragraph 11.1;

"Social Media Incident"	shall mean a post or series of posts that expose Authority Information including information about the Authority's clients or colleagues to unauthorised individuals and/or damages the reputation of the Authority;
"Standards"	shall mean any standards reasonably applicable given the Supplier's expertise and the Services provided, which shall always include as a minimum: 1. G Toolkit or any replacement of the same (if any access to PID or Authority systems/services is required); 2. SO/IEC 27000 series of Information Security Management standards; 3. SO20000; 4. Cyber Essentials; 5. 0 Steps to Cyber Security 6. National Data Guardian data security report/standards/recommendations; 7. CSC – Cloud Security principles; and 8. SO 15489
"Supplier Group"	the Supplier and any of its subsidiaries, with subsidiaries having the meaning defined by section 1159 of the Companies Act 2006 (or any statutory modification or re-enactment of that Act) but for the purposes of section 1159(1) Companies Act 2006 a company shall be treated as a member of another if any shares in that other company are registered in the name of (i) a person by way of security (where the company has provided the security); or (ii) a person as nominee for the company;
"Threat and/or Threat Mitigation Strategy"	shall mean as defined in paragraph 2.2.15;

Traffic	shall mean internet traffic or other communication;
"Traffic Capture"	shall mean the action that may be undertaken during a DDoS Attack to use devices on the relevant network to assist the parties to analyse and investigate that event and thereby assist in informing the Authority of the appropriate countermeasures to undertake;
"User ID"	shall mean as defined in paragraph 8.3.1.

1 GENERAL SECURITY OBLIGATIONS

1.1 Except as strictly required to provide the Services in accordance with the terms of this Agreement or as otherwise agreed, the Supplier shall not:

1.1.1 Undertake any Processing or otherwise make use of Authority Information or Authority System or Authority Records for any other purpose;

1.1.2 purport to sell, let for hire, assign rights in, declare a trust of or otherwise dispose of or commercially exploit any Authority Information;

1.1.3 make any Authority Information or Authority Records available to any third party; or

1.1.4 intercept, analyse or otherwise monitor the traffic which passes through the Authority System.

2 POLICY REQUIREMENTS

2.1 The Supplier will, within 14 days of the commencement of the Term, evidence existing security and cyber policy/policies or, develop, implement and maintain a security and cyber policy/policies (referred to as the Security and Cyber Policy), containing security and cyber procedures relevant to the performance of the Services, including those for the Authority. The Supplier's Security and Cyber Policy shall be designed to protect Authority Information, Authority Records and Authority Systems and shall be periodically updated and audited in accordance with this Schedule **("Security and Cyber Policy"**). The Security and Cyber Policy will set out the security and cyber measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of each element of the Services (both physical and logical) and shall at all times comply with and specify security and cyber measures and procedures which are sufficient to ensure that the

Supplier and each of its Sub-contractors complies with its obligations in accordance with this Schedule. The Supplier shall submit the Security and Cyber Policy not less than annually to the Authority for review. Link: https://www.igt.hscic.gov.uk/

2.2 The Security and Cyber Policy shall include, without limitation, the following security and cyber measures and procedures:

2.2.1 the security and cyber awareness programme provided by the Supplier for Supplier Personnel and its Sub-contractors;

2.2.2 the controls in place to detect any Security and Cyber Incident;

2.2.3 details of vetting procedures undertaken by the Supplier on Supplier Personnel and Sub-contractor personnel who have access to Authority Information, the Authority System or Authority Records;

2.2.4 the procedures to be followed in the event of a breach of the Security and Cyber Policy by Supplier Personnel and/or Sub-contractor Supplier Personnel;

2.2.5 the risk related countermeasures in place to fulfil paragraph 12.3;

2.2.6 (without prejudice to any right of the Authority to approve or reject the use of Sub-contractors) details of the security and cyber arrangements at any Sub-contractor premises used in the performance of the Supplier's obligations under this Agreement;

2.2.7 the Supplier's control for preventing any unauthorised use, alteration or destruction of Authority Information and Authority Records by Supplier Personnel, a Sub-contractor or by any other party;

2.2.8 the Supplier's encryption controls for protecting Authority Information, in line with the Standards;

2.2.9 physical and logical access, including the following:

2.2.9.1 restricting access to Authority Information in any shared environment such that any person who is not authorised by the Authority to do so, may not gain such access;

2.2.9.2 the logical access controls in place to protect information from unauthorised access including, without limitation, limiting the access assigned to users to control their capabilities, and providing access only where authorised;

2.2.9.3 ensure that any Authority Information stored on the Supplier's systems are logically separated from the Supplier's own data and the data of any other party;

2.2.10 the Supplier's preventative, detective and remediation requirements to safeguard the Authority System from vulnerabilities and Malware introduced by Supplier Personnel, a Sub-contractor or by any other party;

2.2.11 the Supplier's anti-virus software, other security and cyber software controls (such as firewalls, anti-Malware, intrusion detection);

2.2.12 the security and cyber testing policy for web sites hosted by the Supplier;

2.2.13 the Supplier's controls for testing and applying security patches;

2.2.14 the Supplier's system development and testing controls; and

2.2.15 a robust and up to date framework, strategy and tools in place to prevent, detect and respond to known and emerging Threats ("Threat Mitigation Strategy"). The Threat Mitigation Strategy must document, require and provide for each of the following that:

2.2.15.1 the Supplier must maintain active and ongoing monitoring for Cyber Attacks;

2.2.15.2 the Supplier must maintain the ability to identify and remove Malicious Traffic in transit prior to such Malicious Traffic reaching any part of the Supplier System or Authority System, without having any material adverse impact upon other Traffic or the Services;

2.2.15.3 the Supplier must maintain the ability to intercept and capture samples of Malicious Traffic and other Traffic Capture activities;

2.2.15.4 the Supplier must maintain the ability to report upon Cyber Attack characteristics in accordance with paragraphs 4 and 6;

2.2.15.5 the Supplier must include an incident response process, in accordance with paragraph 6; and

2.2.15.6 the Supplier must be appropriately scaled to avoid or mitigate the impacts of a Cyber Attack immediately upon occurrence and for the duration of the Cyber Attack and must be capable of providing the Required DDoS Filtering Capacity at all times.

2.3 The measures employed in respect of the Threat Mitigation Strategy must accord with the requirements set out in this Schedule in full, whether or not the Authority has reviewed and approved the Security and Cyber Policy, and without limitation must meet or exceed Good Industry Practice. This may (for example) include but is not limited to entailing the use of automatic Border Gateway Protocol-triggered traffic 'blackholing', scrubbing, dynamic packet inspection and filtering, real-time threat intelligence and/or other appropriate techniques.

2.4 The Supplier acknowledges that:

2.4.1 any Traffic Capture will be deemed the Authority Information for the purposes of this Schedule; and

2.4.2 Traffic and any Traffic Capture may contain Personal Data and shall be processed only in accordance with paragraph 4 of this Schedule.

2.5 Each Party acknowledges that the Supplier may wish to use a Sub-contractor to provide parts of the Threat Mitigation Strategy to filter Malicious Traffic without having any material adverse impact upon other Traffic and/or Services. Without prejudice to the Supplier's requirement to comply with this Schedule, including to maintain the Required DDoS Filtering Capacity, the Supplier shall not engage any Sub-contractor in respect of this requirement without the prior written consent of the Authority in accordance with the terms of this Agreement.

2.6 Immediately following a request by the Authority (or as part of a scheduled audit) the Supplier shall provide the Authority with a copy of the Security and Cyber Policy.

2.7 The Supplier must appoint an accountable senior executive to be responsible for the Security and Cyber Policy and ensure it is updated at least annually (or more frequently as it considers it necessary to do so) and must in any event update the Security and Cyber Policy as follows:

2.7.1 if any change to an applicable Law, the Authority Security and Cyber Policies and Rules or any other Authority policy is introduced and such change necessitates a change to the security and cyber measures and procedures required to provide or receive the Services; or

2.7.2 if the Authority reasonably believes that the Security and Cyber Policy is inconsistent with any

2.8 The Supplier shall appoint a member of Supplier Personnel to be responsible for Security and Cyber Policy compliance within the Supplier's organisation. The responsible member of the Supplier Personnel shall ensure that:

2.8.1 all Supplier Personnel and Sub-contractors understand the process and conditions under which they should, or are required to, invoke and execute the Security and Cyber Incident

Management Procedures; and

2.8.2 Supplier Personnel are aware of when they should escalate Security and Cyber Incidents to their senior managers so as to promote active communication, even on issues of relatively minor concern.

2.9 The Security and Cyber Policy should also include specific controls as described in paragraphs 3 to 13 below.

3 TRAINING AND AWARENESS

3.1 The Supplier must provide security and data protection training and awareness as a part of their employee induction process (key elements on start, full training within eight weeks) and ensure it is repeated annually by all Supplier Personnel.

3.2 Where the Supplier provides staff that are working away from Supplier Group premises for a significant portion of their time, they must also complete any security training prescribed by the Authority.

4 INCIDENT MANAGEMENT PLAN AND REPORTING

4.1 The Supplier shall provide the Authority with a copy of the Incident Management Plan. The parties will agree the relevant operational details from time to time, as soon as reasonably practicable after the Effective Date and in any event within six months of the Effective Date. Once agreed, the Supplier shall ensure that any future plans are no less robust than the agreed Incident Management Plan.

4.2 The Supplier shall have in place a reporting process in order to alert the Authority Representative of all Security and Cyber Incidents (including near misses and/or non-Services impacting incidents) which relate to, or have any impact on the Authority and/or its Authority Service Recipients and/or customers. This reporting process will include but will not be limited to reporting on the characteristics of the Security and Cyber Incident e.g. traffic patterns during DDoS Attacks and information on mitigation techniques used and information on the scale and severity of the Security and Cyber Incident.

4.3 Security and Cyber Incidents (including near misses and/or non-Services impacting incidents) must be reported by the Supplier to the Authority as soon as possible but in any case within twenty four hours or the next Working Day where the Security and Cyber Incident has taken place on a non-Working Day. Notwithstanding the foregoing however, where the Security and Cyber Incident is critical or significant in nature (e.g. the Services provided by the Supplier are impacted adversely or are or may be under threat of disruption which could result in the Services being provided to the Authority and/or its Authority Service Recipients being impacted) such Security and Cyber Incidents must be reported to the Authority immediately. Should the Authority need to be contacted during non-Working Days or out of office hours then the Supplier must contact the Incident Management Team on the CareCERT react number (0800 085 6653) or via e-mail on carecert@nhsdigital.nhs.uk. The Supplier shall provide a detailed written report to the Authority as soon as possible but in any case within five Working Days of the Supplier becoming aware of any Security and Cyber Incident which shall include information regarding what Authority Information or Authority Records have been accessed, removed or corrupted.

4.4 Management information on the Supplier's security performance including measures reflecting

Crown Commercial Service

Good Industry Practice in relation to prevention, mitigation and control of Security and Cyber Incidents shall be provided to the Authority Representative at an agreed frequency but no less than annually.

5 CONTINUITY / IT DR

5.1 The Supplier shall provide the Authority with a copy of its IT Disaster Recovery and Business Continuity Policy and IT Disaster Recovery and Business Continuity plans as at the Effective Date. The parties will agree the relevant operational details from time to time, to reflect the Authority's use of those standard plans, as soon as reasonably practicable after the Effective Date and in any event within six months of the Effective Date. Once agreed, the Supplier shall ensure that any future plans are no less robust than the agreed IT Disaster Recovery and Business Continuity plans.

5.2 The Supplier shall put in place the IT Disaster Recovery and Business Continuity arrangements set out in the agreed IT Disaster Recovery and Business Continuity Policy and IT Disaster Recovery and Business Continuity plans with the aim of ensuring the continued performance of the Services in the event of a material disruption to its operations and/or the failure of any of the systems used in connection with the performance of the Services or any other event which results in the Supplier being unable to perform the Services.

5.3 The Supplier shall:

5.3.1 subject to paragraph 5.4, test the IT Disaster Recovery and Business Continuity plans within nine months of the Effective Date of this Agreement and at intervals of no more than twelve months thereafter and shall promptly update the IT Disaster Recovery and Business Continuity Policy and/or IT Disaster Recovery and Business Continuity plans to resolve any non-conformities with its obligations under this Agreement following such testing, confirming:

5.3.1.1 the test encompassed all IT Disaster Recovery and Business Continuity process, policies and procedures related to preparing for recovery or continuation of the Services; and

5.3.1.2 that disaster recovery proving all technology infrastructure critical to the Supplier has been undertaken to the required level of test scope;

5.3.2 ensure, for hosted IT applications/systems used by the Authority, that the system RTOs and RPOs are aligned with the Authority's operational requirements and have been met;

[Drafting Note - This table is not applicable to this Call Off Contract]

AUTHORITY BIA REFERENCE ID	SYSTEM NAME	AUTHORITY BIA AVAILABILITY RATING	RTO	RPO	PROVING FREQUENCY	PRODUCTION RECOVERY INFRASTRUCTURE REQUIREMENT

5.3.3 ensure that IT Disaster Recovery and Business Continuity plans that have been updated to account for any Change management project activities implemented in the previous twelve (12) months have ensured that RTOs and RPOs, aligned to the Authority's operational requirements, can continue to be met in the event of a disaster scenario;

5.3.4 give the Authority at least two months' notice in writing to allow the Authority to participate (where technically or feasibly possible) in any such testing of the IT Disaster Recovery and Business Continuity plans on the target recovery infrastructure to assure the Authority's connectivity and IT system functionality at the secondary site;

5.3.5 ensure that Business Continuity strategies provide for activation of solutions within the Authority's recovery timescales where as a result of a Security and Cyber Incident there is a:

5.3.5.1 denial of people and premises (i.e. where people / premises cannot be accessed);

5.3.5.2 denial of technology data/information and telecommunications required to perform operations; and

5.3.5.3 disruption to the Supplier's own supply chain dependencies;

5.3.6 ensure that disaster recovery proving takes place immediately after the delivery of new implementations and major changes to the hosted application / systems before going live;

5.3.7 give the Authority such reasonable notice in writing as allows the Authority to be present to witness any such testing of the IT Disaster Recovery and Business Continuity plans in accordance with this paragraph 5 and without prejudice to the above, shall implement any changes reasonably required by the Authority following such testing witnessed by the Authority, in accordance with the Change Control Procedure; and

5.3.8 ensure that the controls and facilities are in place (including reserve power supply and protection against natural hazards) to support Business Continuity planning, disaster recovery and overall back up procedures.

5.4 Where the Authority is satisfied by the Supplier submitting relevant documented submissions that testing referred to in paragraph 5.3.1 would be passed if undertaken and accordingly is not required, the Authority reserves the right to waive any of the requirements in paragraph 5.3.1.

6 INCIDENT MANAGEMENT

6.1 The Supplier must include in the Security and Cyber Policy a procedure ("Security and Cyber Incident Management Procedure") for identifying, preventing, monitoring, reporting and responding to:

6.1.1 the introduction and/or presence of any Malware;

6.1.2 all known and emerging security and cyber incidents including without limitation crime (e.g. theft of property or data); actual or attempted fraud (external and internal employee fraud); unauthorised access to Authority Information, data and / or Authority Systems; Cyber Attacks including DDoS Attacks; physical security breaches and cyber breaches compromising or breaching the security of Authority Information/data/systems and/or involving data leakage and/or data corruption; any incidents which risk impacting the provision of Services to the Authority;

6.1.3 any observed or suspected security and cyber risks or security and cyber incidents in any Supplier System or Supplier network that interconnects with the Authority infrastructure or material Supplier infrastructure (where this is applicable), or that retains Authority Information or Authority Records;

6.1.4 any observed or suspected security and cyber risks or security and cyber incidents in the Authority infrastructure or material Supplier infrastructure including any that interconnects with any other Supplier System or third party system or network as a result of that interconnectivity (where this is applicable);

6.1.5 any incident resulting in or potentially resulting in loss of Authority Records or interruption to business or IT continuity;

6.1.6 any incident that may be indicative of larger, adverse security or cyber related events (for example, DDoS Attacks or Malware penetration) that the Supplier discovers or becomes aware of during the provision of the Services; and

6.1.7 any actual or attempted unauthorised access to or use of any of the Authority infrastructure or material Supplier infrastructure, Authority Information, Authority Records or any sites, facilities, systems or other premises of the Supplier used to provide the Services to the Authority, each of which in paragraphs 6.1.1 to 6.1.7 (inclusive) is a **"Security and Cyber Incident".**

6.2 The Security and Cyber Incident Management Procedure shall detail the following obligations of the Supplier, all of which shall be invoked upon the Supplier becoming aware of a Security and Cyber Incident, where it relates to any aspects of the Services the Supplier shall:

6.2.1 take all steps necessary to remedy such Security and Cyber Incident and/or to protect Information, infrastructure and Authority Records against any Security and Cyber Incident within agreed service levels specified within this Agreement;

6.2.2 take all steps necessary to prevent a similar Security and Cyber Incident in the future;

6.2.3 where appropriate, support the recovery process via all reasonable means (whether the incident relates to data or financial loss);

6.2.4 provide relevant findings from any internal investigations, or take all reasonable steps necessary to provide any assistance to any investigation that the Authority or a third party (appointed by the Authority) requires, including making employees available for interview by the Authority or its appointed third party and supporting any referral to a law enforcement agency or regulator;

6.2.5 at the Authority's request, return to the Authority or the relevant Authority Service Recipients any Authority Information or Authority Records in the Supplier's or its Sub-contractor's possession;

6.2.6 where the Security and Cyber Incident relates to the Authority infrastructure, comply with all reasonable directions of the Authority or the relevant Authority Service Recipients in connection with the remedy of the breach and/or protection of the Authority infrastructure; and

6.2.7 provide the Authority in writing with full details of the steps taken to remedy each actual, potential, threatened or attempted Security and Cyber Incident.

6.3 For situations that do not fall within the Security and Cyber Incidents definitions in this Schedule but where the Authority's reputation in the eyes of any law enforcement agency, regulator or the media is in the Authority's reasonable opinion likely to be damaged, the Supplier must follow the provisions of paragraph 4 and be prepared to follow any guidance from the Authority as to what actions should be taken.

6.4 The Authority retains / maintains the right to pursue both civil and criminal recovery against the Supplier separately or at the same time at the Authority's discretion to cover any losses incurred as a result of any Security and Cyber Incident, including ones arising in the circumstances described in paragraph 7.5.

7 INFORMATION AND CYBER SECURITY

7.1 The Supplier must protect Authority Information throughout its lifecycle and shall maintain an inventory of Authority Information in the Supplier's possession in accordance with the data classification and handling requirements as notified to the Supplier by the Authority from time to time. The Supplier relationship manager in the Authority must be notified promptly where the Supplier requires clarification on how to handle Authority Information.

7.2 Where the Supplier hosts a web site containing Authority Information or displays the Authority branding, the Supplier shall agree with the Authority the following requirements:

7.2.1 the security testing to be performed by a skilled independent service provider who is accredited to an industry recognised security testing body (CREST) prior to the pages being hosted on the Internet. The times and dates of the security testing are to be agreed by mutual consent of both parties; and

7.2.2 a regular security testing schedule of the web site at a frequency as agreed with the Authority.

7.3 Where the Supplier is involved in any software development, the Supplier shall follow secure development practices in accordance with Good industry Practice, including without limitation ensuring that all developers are skilled and trained in relevant secure development practices and integrating appropriate security practices and testing into the software development lifecycle.

7.4 Where a significant change may affect the provision of Services or Authority Information, Records or data, the Supplier shall give the Authority not less than twenty eight days' notice of the proposed changes in order that a security test may be arranged subject to 7.2 above.

7.5 Where a vulnerability is identified in a Supplier's System that hosts or supports Authority Information and processes it shall be remediated expeditiously by the Supplier and in any event within the timescales specified by the Authority. The Supplier shall amongst other things be liable to the Authority for any losses suffered by the Authority [or any Authority Service Recipient] resulting from either an unpatched or an unsupported element of the Supplier System where an update or a patch was made available at least 5 Working Days prior to the Cyber and Security Incident causing the loss.

7.6 The Supplier shall not introduce or permit the introduction of any Malware or vulnerabilities into, or be the source of any malicious activity against, any of the Authority's infrastructure (for example, Malware, spamming or denial-of-service attack). Where any Malware or vulnerability is identified by the Supplier which may pose an actual or potential threat to the Authority or the

Supplier, the Supplier shall promptly notify the Authority of the same and provide details in writing of any such Malware or vulnerabilities to the Authority, including the Supplier's proposed remediation plan, or actions taken in response.

7.7 If Malware or a vulnerability is introduced on to the Authority System by a member of Supplier Personnel or Sub-contractor, the Supplier shall reimburse the Authority for the costs and expenses that arise as a consequence of the Authority taking all actions required to remediate the vulnerability.

7.8 The Supplier shall not, without the prior written consent of the Authority Representative (authorised to provide such consent under this Agreement) insert or allow the insertion of any code that would disable, shut down or otherwise materially adversely impact all or any portion of the Authority's infrastructure.

8 DATA SECURITY AND LOGICAL ACCESS CONTROL

8.1 The Supplier shall hold no Authority Information or Authority Records on any portable device in any media (including but not limited to a laptop, CD, USB memory stick and all other similar media). Should the Supplier require use of any portable devices, in any media (including but not limited to a laptop, CD, USB memory stick, back up tapes and all other similar media) in order to deliver the Services to the Authority the Supplier shall:

8.1.1 ensure all Authority Information and Authority Records held on any such portable device are encrypted in accordance with Good Industry Practice and in accordance with the Authority's requirements (which include the Approved Cryptographic Algorithms Good Practice Guideline) as notified to the Supplier from time to time;

8.1.2 request written approval by the Authority for each type of portable device in any media (including but not limited to a laptop, CD, USB memory stick, back up tapes and all other similar media); and

8.1.3 immediately notify the Authority in the event that any Authority Information or Authority Records have been accessed through an un-encrypted device, in accordance with paragraph 4 of this Schedule.

8.2 Subject to paragraph 8.1, the Authority hereby gives such consent to the Supplier to hold and process encrypted Authority Information and Authority Records on laptops. The Supplier will immediately notify and request written approval from the Authority in the event of any changes to its encryption process or other security facilities of all such devices, including assessment of these changes and whether they are in accordance with both Good Industry Practice and in accordance with the Authority's requirements. For the avoidance of doubt the Authority maintains all rights to withdraw any consent, and will provide such notice in writing in the event of the Supplier breaching any data protection or security requirements, as detailed within this Schedule. Should such consent be withdrawn by the Authority the Supplier will immediately remove, destroy, and decommission all of the Authority Information and the Authority Records in accordance with this Schedule from any device where such consent has previously been provided.

8.3 The Supplier shall not access the Authority infrastructure and/or the Authority Information on the Authority infrastructure and/or access the Authority's assets without the prior written consent of the Authority, which consent may be withheld in the Authority's absolute discretion. If the Supplier requests such consent and such consent is given, the Supplier shall comply with the Authority's infrastructure security and cyber measures as detailed in the Authority Security

and Cyber Policies and Rules to guard against any unauthorised access to, and against any alteration or destruction of, the Authority infrastructure and/or Data stored on such system. At the Effective Date, these measures require, as a minimum, that:

8.3.1 all Supplier Personnel and Sub-contractors hold a unique user identification number ("User ID") and strong password (such password shall meet the requirements set out in the Approved Cryptographic Algorithms Good Practice Guideline) prior to gaining access to the Authority infrastructure. The Supplier shall apply to the Authority for User IDs for all Supplier Personnel and Sub-contractors who require access to the Authority infrastructure. Grant of such applications shall be at the sole discretion of the Authority;

8.3.2 where a Supplier Employee or Sub-contractor has been supplied with a PC, laptop or other device by the Authority all Supplier Group Policies must be complied with, including not transmitting the Authority Information or the Authority Records from the Authority email address to the Supplier's infrastructure or any other external email accounts without prior written consent of an Authority representative (authorised to provide such consent under this Agreement);

8.3.3 the Supplier complies and observes all parameters that control user access to areas and features of the Authority's infrastructure;

8.3.4 the Supplier shall ensure that all Supplier Personnel or Sub-contractors are aware that any User IDs (or accounts) issued by the Authority for the performance of the Services, passwords and security tokens, including ID cards, associated with User IDs (or accounts) shall not be disclosed or shared with any other individual (either internally or externally to the Authority or the Supplier);

8.3.5 the Supplier shall have processes to identify any Supplier Personnel or Sub-contractors who no longer require access to the Authority's infrastructure (due to leaving or being no longer involved in the provision of Services). The processes must include:

8.3.6 timely identification of job role changes or leavers to meet the notification requirements of paragraph 8.3.8;

8.3.7 that recertifications of Supplier Personnel or Sub-contractors' access to the Authority's infrastructure are performed on a quarterly basis;

8.3.8 timely notification to the Authority if any Supplier Personnel or Sub-contractor no longer requires access to the Authority's infrastructure, to enable the Authority to remove the relevant access authority, including the relevant User IDs and passwords. The Supplier will ensure that any security token or ID card is returned to the Authority immediately following the date on which any Supplier Personnel or Sub-contractor no longer requires access to the Authority's infrastructure; and

8.3.9 that all Supplier Personnel and Sub-contractors are aware that the Authority may monitor the Supplier Personnel's and Sub-contractors' use of the Authority's infrastructure (including routine monitoring of e-mail and internet usage, contents and traffic).

8.4 The Supplier shall provide ACLs (Access Control Lists) to the Authority for all Authority Users on a quarterly basis for systems and applications under the Supplier's management. The ACL must include the user identifier and associated access permissions.

8.5 The Supplier shall implement a password policy for systems and applications under the Supplier's management in line with Good Industry Practice.

Crown Commercial Service

9 PHYSICAL AND PEOPLE SECURITY

Appointed Person

9.1 The Supplier shall have a nominated person who is responsible for physical security provision and ensures that compliance with the following requirements is achieved.

Security Review and Assessment

9.2 The Supplier must ensure that a general security review of all premises from which the Authority's activity / data storage etc. is conducted should be undertaken at least annually, or whenever there is significant change to the Services provided or premises operated from.

9.3 These reviews should be provided to the Authority Representative and the Authority's Group Security and Fraud team on request.

9.4 The Supplier shall alert the Authority Representative within twenty four hours of the discovery of any identified physical security issues.

Physical Security Provision

9.5 The Supplier must implement appropriate risk related countermeasures to:

9.5.1 ensure the Supplier's premises are protected, to an agreed level, against unauthorised access, intrusion, or damage due to a Security and Cyber Incident;

9.5.2 minimise the probability of an interruption to Supplier's business operations and Services provided to the Authority and its Authority Service Recipients from a Security and Cyber Incident;

9.5.3 minimise the probability of a compromise of, damage to, or loss of, or removal of, the Authority's assets from a criminal, malicious, or negligent act; and

9.5.4 protect to agreed levels, the confidentiality, integrity and availability of the Authority Information.

9.6 To achieve the above measures, the Supplier shall as a minimum:

9.6.1 have an appropriate and auditable access control system in place to ensure only authorised personnel are permitted to enter the Supplier's premises;

9.6.2 have robust visitor management processes in place to ensure all visitors are logged and supervised. The logs must be retained for twelve months;

9.6.3 deploy CCTV to monitor and record premises' entry/exit points and secure areas;

9.6.4 CCTV images should be stored for a minimum of thirty days, or where data is stored or is governed by specific regulations such as PCI-DSS, this retention period should be ninety days;

9.6.5 have an intrusion detection system that is monitored either on site or by an appropriate alarm receiving centre operating 24 hours a day, 7 days a week, 365 days a year; and

9.6.6 maintain electronic security systems by use of an approved (NSI Gold or equivalent) installation and maintenance company.

Records Management

9.7 The Supplier will develop, implement and maintain a records policy containing mandatory requirements to ensure all records, in all formats/media, including electronic and physical in any location (including the Supplier Group records) are managed appropriately by the Supplier throughout their lifecycle. Such records policy (the "Records Policy") will align to the Standards as a minimum.

9.8 The Records Policy shall be periodically updated (every twelve months as a minimum) and audited in accordance with any audit provisions set out elsewhere in this Agreement.

9.9 The Records Policy will ensure that the Supplier and its Sub-contractors comply with their obligations to the Authority.

9.10 The Supplier and its Sub-contractors will ensure that they have sufficient processes, plans and procedures in place to carry out control testing and ongoing monitoring to ensure compliance with their Records Policy and to ensure any records related incidents, risks or breaches are identified, reported and handled promptly and appropriately.

9.11 The Supplier and its Sub-contractors will not transfer, store or access any Authority Records outside the European Economic Area (EEA), either through direct transfer or via remote access (e.g. via outsourcing, as part of business continuity arrangements, via cloud arrangements, via offshore service models, etc.) without the prior written consent of the Authority. Where such consent is given, it will be conditional upon the Supplier complying with any controls on the transfer of Personal Data set out in clause 3 of this Order Form.

9.12 The Supplier and its Sub-contractors will ensure they have a risk management process that enables the identification and management of records management risks.

9.13 The Supplier and its Sub-contractors will report any material records breaches, incidents or risks to the Authority without undue delay and in any event, within 24 hours.

9.14 The Supplier will provide adequate records management training, at least annually, for the Supplier Personnel and its Sub-contractors, with evidence of completion.

9.15 The Supplier will maintain a record inventory for all the Authority Records which are created, received, stored, processed or destroyed by the Supplier and its Sub-contractors. The record inventory will be reviewed regularly (every six months as a minimum) and updated accordingly.

9.16 The Supplier and its Sub-contractors will securely store and protect the Authority Records in accordance with the provisions of this Schedule.

9.17 The Supplier and its Sub-contractors will securely store the Authority Records in an appropriate format and location to ensure the records are reliable, usable and can be read and retrieved over time.

9.18 The Supplier and its Sub-contractors will agree a process to enable the Authority to retrieve any Authority Records within agreed timescales to fulfil legal, regulatory, Authority or business requirements.

9.19 The Supplier and its Sub-contractors will retain all the Authority Records for a specific period of time in line with the Authority Policies, appropriate record retention practices and, where applicable, with Data Protection Laws.

9.20 The Supplier and its Sub-contractors will agree an authorisation process with the Authority for the secure destruction of the Authority Records. The Supplier and its Sub-contractors will retain documented evidence of the authorisation and secure record destruction.

9.21 The Supplier and its Sub-contractors must ensure they can apply legal holds to prevent destruction of the Authority Records. A process must be agreed with the Authority to apply legal holds to any records (electronic and physical) being managed by the Supplier and its Sub-contractors upon notification from the Authority.

10 SOCIAL MEDIA

10.1 The Authority Information, which the Supplier is responsible for, must be protected by the

Supplier throughout its lifecycle. This includes the posting of the Authority Information by the Supplier Personnel on personal or Supplier owned social media channels/accounts.

10.2 The Supplier shall ensure that the Supplier Personnel protect the Authority and its Authority Service Recipients by only disclosing publicly available information about the Authority and its Authority Service Recipients.

10.3 The Supplier shall ensure that Supplier Personnel shall not:

10.3.1 make reference to the Authority's business information (including key IT systems and processes) or dealings relating to the Authority's colleagues, customers, clients, partners, or suppliers;

10.3.2 post opinions on personal social media accounts, which could reasonably be construed as official comment on behalf of the Authority;

10.3.3 post anything about the Authority, its customers, clients or colleagues containing abusive, obscene or libellous comments; or

10.3.4 use the NHS logo, associated brands (e.g. NHS Digital) or trademarks on social media channels without approval.

10.4 The Supplier must ensure that:

10.4.1 Supplier Personnel have undertaken and understood the requirements set out in social media awareness training;

10.4.2 any exceptions to the ordinary use of social media in relation to this Agreement must be raised with the Authority Representative and have prior written agreement from the Authority; and

10.4.3 Social Media Incidents are reported to the Authority Representative.

11 SECURITY AUDITS

11.1 The Authority reserves the right to inspect any aspect of the security arrangements and processes relating to the Supplier's and/or its Sub-contractors' provision of the Services and its Processing of Personal Data (including the Supplier's and/or its Sub-contractors' security environment, arrangements, policies, training arrangements for staff and processes used in the performance of the Services) ("Security Audits") once in each twelve (12) month period during the Term of the Agreement. Where the Supplier has performed independent reviews of Sub-contractors and is able to share these findings, these will be taken into consideration during the Security Audit. The Authority shall also have the right to conduct additional Security Audits in the following circumstances:

11.1.1 if the Authority considers it necessary to do so to satisfy applicable Law or local or national regulation;

11.1.2 following an actual or potential Security and Cyber Incident or Personal Data Breach or becoming aware of any actual or potential threat;

11.1.3 if a Security Audit reveals a deficiency in the Security and Cyber Policy;

11.1.4 if the Authority acting reasonably believes that the Supplier has failed to provide the Services in accordance with the security measures and obligations imposed on the Supplier under this Schedule and any solutions provided by the Supplier from time to in accordance with paragraph 11.4; and

11.1.5 where the provisions of paragraph 12 apply.

11.2 Security Audits may include tests designed to breach the protections set out in the Security and Cyber Policy and associated security measures (including security penetration testing) and shall be conducted with no less than ten days' prior written notice. Security Audits may also require the Supplier to demonstrate their capability in providing the Services on an uninterrupted or otherwise unaffected basis in the event of Security and Cyber Incidents.

11.3 The Supplier shall make available to the Authority, at the request of the Authority and where the Authority's Information is hosted any Supplier computer systems, Supplier Personnel to assist in any Security Audit and the Supplier will co-operate fully with any investigation relating to their operations.

11.4 If the Authority reasonably believes that the results of a Security Audit identify a weakness in the security measures adopted by the Supplier, the Supplier shall evaluate such weakness and provide a suitable solution to the Authority's satisfaction within timescales agreed by the Authority. The results of any Security Audit and any solution provided pursuant to this paragraph shall be without prejudice to the Supplier's obligations in this Agreement.

11.5 Following a Security Audit:

11.5.1 the Authority may conduct an exit conference with the Supplier to confirm material facts identified in the Security Audit; and

11.5.2 if a Security Audit demonstrates that the Supplier is failing to comply with this Agreement, the Supplier shall promptly take any steps which the Authority, acting reasonably, determines are necessary for it to comply with this Agreement within the timescales as required by the Authority.

11.6 Where the Supplier receives notice from a regulator that a regulatory audit or investigation is to be carried out in respect of the Supplier's business or affairs the Supplier shall inform the Authority of such notice as soon as is reasonably practicable.

12 STORAGE AND DESTRUCTION OF THE AUTHORITY INFORMATION

12.1 The Supplier shall protect all the Authority Information (held by Supplier Personnel or Sub-contractors in any form) by adopting a 'clear desk' policy in respect of the Authority Information and disposing of such the Authority Information securely by treating it as confidential waste.

12.2 The Supplier shall provide Supplier Personnel and procure that Sub-contractors provide their employees with:

12.2.1 locking filing cabinets to house any Authority Information when such is not in use; and

12.2.2 facilities for the secure disposal of the Authority Information.

12.3 The Supplier shall ensure that any of the Authority Information held by the Supplier or a Sub-contractor is disposed of by or on behalf of the Supplier or Sub-contractor in a manner which protects the confidential nature of the Authority Information and in compliance with this paragraph of this Schedule.

13 TERMINATION AND DECOMMISSIONING

At the end of the Term (for whatever reason) the Supplier must ensure that:

13.1 where required by the Authority or as may otherwise be necessary, a continuing confidentiality undertaking and (if Personal Data is involved) data processing agreement by the Supplier, its

employees and its Sub-contractors remains in force regarding the Authority Records, the Authority Information and the Authority infrastructure, on an ongoing basis;

13.2 upon exit all physical access rights to any NHS Digital and/or any Authority Service Recipients' premises by the Supplier and its Sub-contractors shall be revoked and the means of access to sites or security systems (e.g. access passes or keys) must be returned to the Authority within 24 hours;

13.3 in addition to the requirements already set out above where the Authority requires, the Authority Information and the Authority Records must be returned to the Authority in a mutually agreed format;

13.4 where the Authority does not require the return of the Authority Information and the Authority Records these must be securely and irrevocably deleted or disposed of by or on behalf of the Supplier and all Sub-contractors in accordance with applicable Law, Standards and in a manner consistent with the Authority Policies and any requirements notified to the Supplier from time to time;

13.5 if the Supplier is required to retain the Authority Information or the Authority Records for legal or regulatory purposes, the Authority must approve the request and measures implemented to ensure the correct storage and destruction of this information at the end of such retention period;

13.6 in the event that the Authority Information or the Authority Records cannot be retrieved / deleted without compromising the integrity of information retained by the Supplier and/or its Sub-contractors:

13.6.1 each party acknowledges that, due to the nature of their respective operations, each party has a standard data archiving policy which includes the creation and retention of backup copies of Data and other information ("Retained Data") held on its computer systems for legal/regulatory compliance, IT restoration and disaster recovery purposes only. Each party therefore agrees that (subject to paragraph 13.6.2 below) the Retained Data held by the other party shall not be subject to an obligation to be returned or deleted, whether at the end of the Term or otherwise. For the avoidance of doubt:

13.6.1.1 to the extent that the Retained Data contains data supplied to one party by the other party, it shall remain subject to the other terms of this Agreement as may be applicable; and

13.6.1.2 to the extent that the Retained Data contains Supplier output or information derived from it, such data may not be used by the Authority for live operational purposes after the end of the Term unless expressly provided for in the Agreement;

13.6.2 if and to the extent that the Supplier is expressly stated within any agreement to be acting as a Data Processor on behalf of the Authority then:

13.6.2.1 the Supplier shall ensure that those Authority Records to be Processed by the Supplier under such specific agreement are disposed of by or on behalf of the Supplier in accordance with applicable Law and in a manner consistent with the Authority Policies and any requirements notified to the Supplier from time to time; and

13.6.2.2 the Supplier shall ensure that those Authority Records to be Processed by the Supplier under such specific agreement are readable, retrievable and reproducible during their lifetime and that appropriate controls are put in place to ensure the authenticity and integrity of those Authority Records; and

13.6.3 the Authority retains the rights as detailed this paragraph in the event that any Security and

Crown Commercial Service

Cyber Incident not previously identified becomes apparent.

Crown Commercial Service

APPENDIX 1

Approved Cryptographic Algorithms Good Practice Guideline

Approved
Cryptographic Algorit