

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	C244015
THE BUYER:	NHS England
BUYER ADDRESS	7-8 Wellington Place, Leeds, LS1 4AP
THE SUPPLIER:	Softcat Plc
SUPPLIER ADDRESS:	Solar House, Field Lane, Marlow, SL71 LW
REGISTRATION NUMBER:	02174990
DUNS NUMBER:	397333253

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 19th June 2024.

It's issued under the Framework Contract with the reference number RM6098 for the provision of Technology Products & Associated Service.

CALL-OFF LOT(S):

Lot 3 Software

CALL-OFF INCORPORATED TERMS

This is a Bronze Contract.

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form, including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM6098
3. Framework Special Terms

RM6098 Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

4. The following Schedules in equal order of precedence:

- Joint Schedules for RM6098
 - Joint Schedule 2 (Variation Form)
 - Joint Schedule 3 (Insurance Requirements)
 - Joint Schedule 4 (Commercially Sensitive Information)
 - Joint Schedule 6 (Key Subcontractors)
 - Joint Schedule 7 (Financial Difficulties)

 - Joint Schedule 10 (Rectification Plan)
 - Joint Schedule 11 (Processing Data)
- Call-Off Schedules for C244015
 - Call-Off Schedule 5 (Pricing Details)
 - Call-Off Schedules 6 (ICT Services) including Annexes A to E
 - Call-Off Schedule 8 (Business Continuity and Disaster Recovery) [amended for a Bronze Contract as per paragraph 10 of Part A of that Schedule]
 - Call-Off Schedule 9 (Security) Part A: short form security requirements and Part B annex 1
 -
 - Call-Off Schedule 15 (Call-Off Contract Management)
 - Call-Off Schedule 16 (Benchmarking)
 - Call-Off Schedule 20 (Call-Off Specification)

5. CCS Core Terms (version 3.0.11) as amended by the Framework Award Form

6. Joint Schedule 5 (Corporate Social Responsibility) RM6098

7. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract:

Special Term 1: Cyber Security Requirements

The following wording shall be included as a new Clause 3.4 of the Core Terms of the Call-Off Contract:

RM6098 Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

The Supplier warrants and represents that it has complied with and throughout the Contract Period will continue to comply with the Cyber Security Requirements. The “**Cyber Security Requirements**” means:

- a) compliance with the data security and protection toolkit (DSP 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 Buyer or the Department of Health and Social Care from time to time;
- b) such requirements as are identified by the Buyer in its Security Policy (if applicable); and
- c) any other cyber security requirements relating to the Services notified to the Supplier by the Buyer from time to time;

Special Term 2: Supplier Staff

The following wording shall be included as a new Clause 7.6 of the Core Terms of the Call-Off Contract:

7.6 Call-Off Schedule 9 (Security) has been incorporated into this Order Form under the section headed “CALL-OFF INCORPORATED TERMS”, and paragraph 3.4.3 of Part B of Call-Off Schedule 9 (Security) shall also apply to this Order Form .

7.7 ISO/IEC27001 and ISO/IEC27002 or equivalent standard, such as Cyber Essentials Plus.

Special Term 3: Intellectual Property Rights (IPRs)

Clause 9.1 of the Core Terms of the Call-Off Contract – Delete this Clause and replace with:

9.1. Each Party keeps ownership of its own Existing IPRs. Any New IPR created under a Contract is owned by the Buyer. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier’s Existing IPR to enable it to:

- receive and use the Deliverables
- make use of the deliverables provided by a Replacement Supplier
- develop and provide products and services to third-parties

9.2 Nothing in this Contract shall be interpreted as the provision of permission by the Buyer to use Government Data or any New IPR derived from Government Data to develop or train AI or machine learning systems.”

RM6098 Framework Schedule 6 (Order Form Template and Call-Off Schedules)
Crown Copyright 2018**Special Term 4: Execution and Counterparts**

The following wording shall be included as new Clause 36 of the Core Terms of the Call-Off Contract:

36 Execution and Counterparts

36.1 This Call-Off 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.

36.2 Execution of this Call-Off 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 Call-Off 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 Call-Off Contract as if signed by each Party's manuscript signature. In such situation, this Call-Off Contract shall be formed on the date on which both Parties have electronically signed the Call-Off Contract as recorded in the Buyer's electronic contract management system.

CALL-OFF START DATE: **1st July 2024**

CALL-OFF EXPIRY DATE: **30th June 2025**

CALL-OFF INITIAL PERIOD: **12 Months**

CALL-OFF OPTIONAL EXTENSION PERIOD **12 Months**

MINIMUM PERIOD OF NOTICE FOR WITHOUT REASON TERMINATION **6 months**

CALL-OFF DELIVERABLES

See details in Call-Off Schedule 20 (Call-Off Specification)

Summary of products

Product / Service	Number	Description
Cyber Professional Licences	Enterprise-wide license	2000+ world leading Cyber Security on demand labs with the catalogue growing weekly

RM6098 Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

		Includes a Customer Success Manager who will support with everyday tasks such as licencing and basic reporting
App Sec Cloud Sec	Enterprise-wide license	The aim is to leverage data insights to strengthen the software development life cycle and reduce vulnerabilities in applications
Crisis Simulation Tool	Enterprise-wide license	Access to a library of cyber incident response scenarios and ability to custom build own scenarios relevant to work area. Catalogue of scenarios is continuously added to
Screening	Enterprise-wide license	Allows managers to effectively tailor job advertisements to specific technical roles and then test candidates' technical ability before interview. For internal or external candidates
Team Sim	10 Credits	Prove the effectiveness of Red and Blue Teams as they progress through complex technical scenarios.
Cyber Workforce Advisor	1 Full Time Dedicated	Full time resource attached to account to drive engagement and ensure successful outcomes. Employed by Immersive Labs, but very much embedded into the NHS

LOCATION FOR DELIVERY

On-line NHS account

DATES FOR DELIVERYDelivery date details: per contract start date 1st July 2024**TESTING OF DELIVERABLES**

NONE

WARRANTY PERIOD

The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall be as per the term of the Contract.

MAXIMUM LIABILITY

RM6098 Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Year 1 Charges used to calculate liability in the first 12 months is **£1,029,236.50** paid up front for the Enterprise licence

The Total Value of the contract over the 2 year term is **£2,058,473.00**
See further details in Order Schedule 5 (Pricing Details)

CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details)

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of a Specific Change in Law or Benchmarking using Call-Off Schedule 16 (Benchmarking) where this is used.

REIMBURSABLE EXPENSES

None other than by separate and specific agreement

PAYMENT METHOD

Payment via BACS within 30 days of invoice

BUYER'S INVOICE ADDRESS:

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

Invoices should clearly quote the purchase order number, be addressed to NHS England, X24 Payables K005, 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, 'X24 Invoice Scanning' in subject line or alternatively invoices can be sent via post to the above address.

BUYER'S AUTHORISED REPRESENTATIVE

[REDACTED]

[REDACTED]

RM6098 Framework Schedule 6 (Order Form Template and Call-Off Schedules)
Crown Copyright 2018

BUYER'S ENVIRONMENTAL POLICY

NHS England Social Value Charter available online at: [NHS England Social value charter](#)

RM6098 Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

&

NHS England's [Sustainable development management plan: summary report](#)

BUYER'S SECURITY POLICY

Call Off Schedule 9 B Part A short form security requirements.

SUPPLIER'S AUTHORISED REPRESENTATIVE

[REDACTED]

SUPPLIER'S CONTRACT MANAGER

[REDACTED]

PROGRESS REPORT FREQUENCY

On the first Working Day of each calendar month

Access

PROGRESS MEETING FREQUENCY

Quarterly on the first Working Day of each quarter or as requested by the Buyer

KEY STAFF

Named account
manager from
Immersive Labs

KEY SUBCONTRACTOR(S)

Immersive Labs

COMMERCIALLY SENSITIVE INFORMATION

Breakdown of Supplier Pricing

SERVICE CREDITS

Not Applicable

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

RM6098 Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

SOCIAL VALUE COMMITMENT

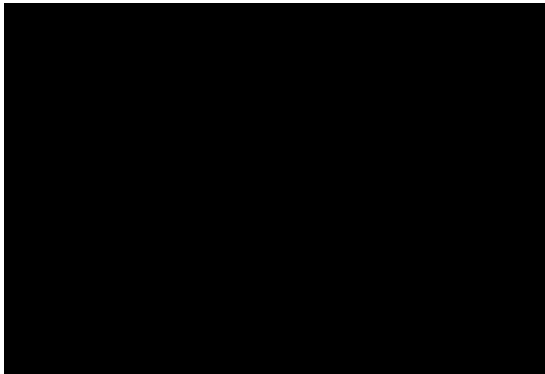
Not applicable

[BUYER CORE GOODS AND/OR SERVICES REQUIREMENTS]**[Goods and/or Services]**

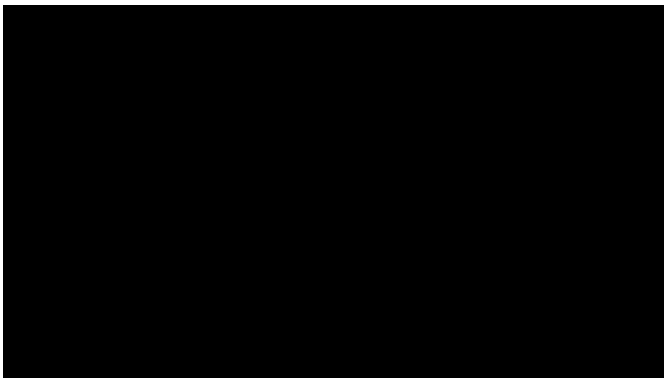
- 1 The following requirements shall take priority above all terms, conditions and specifications set out in this Call-Off Contract (including without limitation any embedded documents and terms), and the Supplier shall ensure that the software licences meet and conform with the following requirements:
 - 1.1 The Buyer shall be entitled, free of charge, to sub licence the software to any contractor and/or sub-contractor of the Buyer who is working towards and/or is providing services to the Buyer.
 - 1.2 The Buyer's role as national information and technology partner to the NHS and social care bodies involves the Buyer 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 Buyer from discharging its role as the national information and technology partner for the health and care system, which includes the ability of the Buyer 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 Buyer's services.
 - 1.3 The Buyer shall be entitled to deploy the software at any location from which the Buyer and/or any contractor and/or sub-contractor of the Buyer is undertaking services pursuant to which the software is being licenced.
 - 1.4 Any software licenced to the Buyer on a named users 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 Subcontractor of the Buyer).
 - 1.5 The Supplier shall ensure that the Buyer 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.
 - 1.6 The Supplier shall notify the Buyer in advance if any software or service permits the Supplier or any third-party remote access to the software or systems of the Buyer.
 - 1.7 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 Buyer.]

RM6098 Framework Schedule 6 (Order Form Template and Call-Off Schedules)
Crown Copyright 2018

For and on behalf of the Supplier:



For and on behalf of the Buyer:



Joint Schedule 1 (Definitions)
Crown Copyright 2018

Joint Schedule 1 (Definitions)

- 1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.
- 1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.
- 1.3 In each Contract, unless the context otherwise requires:
- 1.3.1 the singular includes the plural and vice versa;
 - 1.3.2 reference to a gender includes the other gender and the neuter;
 - 1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Central Government Body;
 - 1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;
 - 1.3.5 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";
 - 1.3.6 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;
 - 1.3.7 references to "**representations**" shall be construed as references to present facts, to "**warranties**" as references to present and future facts and to "**undertakings**" as references to obligations under the Contract;
 - 1.3.8 references to "**Clauses**" and "**Schedules**" are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;
 - 1.3.9 references to "**Paragraphs**" are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;
 - 1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;
 - 1.3.11 the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

1.3.12 where the Buyer is a Central Government Body it shall be treated as contracting with the Crown as a whole;

1.3.13 any reference in a Contract which immediately before Exit Day was a reference to (as it has effect from time to time):

- (a) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement ("**EU References**") which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 shall be read on and after Exit Day as a reference to the EU References as they form part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and
- (b) any EU institution or EU authority or other such EU body shall be read on and after Exit Day as a reference to the UK institution, authority or body to which its functions were transferred; and

1.3.14 unless otherwise provided, references to "**Buyer**" shall be construed as including Exempt Buyers; and

1.3.15 unless otherwise provided, references to "**Call-Off Contract**" and "**Contract**" shall be construed as including Exempt Call-off Contracts.

1.4 In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

Achieve"	in respect of a Test, to successfully pass such Test without any Test Issues and in respect of a Milestone, the issue of a Satisfaction Certificate in respect of that Milestone and " Achieved ", " Achieving " and " Achievement " shall be construed accordingly;
Additional insurances"	insurance requirements relating to a Call-Off Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements);
Admin Fee"	means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees ;
Affected Party"	the Party seeking to claim relief in respect of a Force Majeure Event;
Affiliates"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
Annex"	extra information which supports a Schedule;
Approval"	the prior written consent of the Buyer and " Approve " and " Approved " shall be construed accordingly;
Audit"	the Relevant Authority's right to:

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<ul style="list-style-type: none"> a) verify the accuracy of the Charges and any other amounts payable by a Buyer under a Call-Off Contract (including proposed or actual variations to them in accordance with the Contract); b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services; c) verify the Open Book Data; d) verify the Supplier's and each Subcontractor's compliance with the Contract and applicable Law; e) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations; f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables; g) obtain such information as is necessary to fulfil the Relevant Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract; i) carry out the Relevant Authority's internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts; j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant Authority has used its resources; or k) verify the accuracy and completeness of any Management Information delivered or required by the Framework Contract;
Auditor"	<ul style="list-style-type: none"> a) the Relevant Authority's internal and external auditors; b) the Relevant Authority's statutory or regulatory auditors; c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; d) HM Treasury or the Cabinet Office; e) any party formally appointed by the Relevant Authority to carry out audit or similar review functions; and f) successors or assigns of any of the above;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Authority"	CCS and each Buyer;
Authority Cause"	any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier;
BACS"	the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom;
Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Contract;
Buyer"	the relevant public sector purchaser identified as such in the Order Form;
Buyer Assets"	the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract;
Buyer Authorised representative"	the representative appointed by the Buyer from time to time in relation to the Call-Off Contract initially identified in the Order Form;
Buyer Premises"	premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them);
Call-Off Contract"	the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the Framework Contract), which consists of the terms set out and referred to in the Order Form;
Call-Off Contract period"	the Contract Period in respect of the Call-Off Contract;
Call-Off Expiry Date"	the scheduled date of the end of a Call-Off Contract as stated in the Order Form;
Call-Off incorporated terms"	the contractual terms applicable to the Call-Off Contract specified under the relevant heading in the Order Form;
Call-Off Initial period"	the Initial Period of a Call-Off Contract specified in the Order Form;
Call-Off Optional extension Period"	such period or periods beyond which the Call-Off Initial Period may be extended as specified in the Order Form;
Call-Off procedure"	the process for awarding a Call-Off Contract pursuant to Clause 2 (How the contract works) and Framework Schedule 7 (Call-Off Award Procedure);
Call-Off Special terms"	any additional terms and conditions specified in the Order Form incorporated into the applicable Call-Off Contract;
Call-Off Start Date"	the date of start of a Call-Off Contract as stated in the Order Form;

Framework Ref: RM6098

Project Version: v1.0

Model Version: v3.11

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Call-Off Tender"	the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following a Further Competition Procedure and set out at Call-Off Schedule 4 (Call-Off Tender);
CCS"	the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP;
CCS Authorised representative"	the representative appointed by CCS from time to time in relation to the Framework Contract initially identified in the Framework Award Form;
Central government body"	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;
Change in Law"	any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date;
Change of control"	a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;
Charges"	the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Call-Off Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Call-Off Contract less any Deductions;
Claim"	any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract;
Commercially sensitive information"	the Confidential Information listed in the Framework Award Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
Comparable supply"	the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables;
Compliance officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
Confidential information"	means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	"confidential") or which ought reasonably to be considered to be confidential;
Conflict of interest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS;
Contract"	either the Framework Contract or the Call-Off Contract, as the context requires;
Contract Period"	the term of either a Framework Contract or Call-Off Contract on and from the earlier of the: a) applicable Start Date; or b) the Effective Date up to and including the applicable End Date;
Contract Value"	the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier;
Contract Year"	a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof;
Control"	control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "Controlled" shall be construed accordingly;
Controller"	has the meaning given to it in the UK GDPR;
Core Terms"	CCS' terms and conditions for common goods and services which govern how Suppliers must interact with CCS and Buyers under Framework Contracts and Call-Off Contracts;
Costs"	the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables: a) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Work Day, of engaging the Supplier Staff, including: i) base salary paid to the Supplier Staff; ii) employer's National Insurance contributions; iii) pension contributions; iv) car allowances; v) any other contractual employment benefits; vi) staff training; vii) work place accommodation; viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and ix) reasonable recruitment costs, as agreed with the Buyer;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>b) costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets;</p> <p>c) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables; and</p> <p>d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables;</p> <p>but excluding:</p> <p>e) Overhead;</p> <p>f) financing or similar costs;</p> <p>g) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Call-Off Contract Period whether in relation to Supplier Assets or otherwise;</p> <p>h) taxation;</p> <p>i) fines and penalties;</p> <p>j) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and</p> <p>k) non-cash items (including depreciation, amortisation, impairments and movements in provisions).</p>
CRTPA"	the Contract Rights of Third Parties Act 1999;
"Cyber essentials equivalent"	<p>ISO27001 certification where:</p> <p>a) the Cyber Essentials requirements, at either basic or Plus levels as appropriate, have been included in the scope, and verified as such; and</p> <p>b) the certification body carrying out this verification is approved to issue a Cyber Essentials certificate by one of the accreditation bodies</p> <p>This would be regarded as holding an equivalent standard to Cyber Essentials.</p>
Data Protection Impact assessment"	an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
Data Protection legislation"	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy;
Data Protection liability Cap"	the amount specified in the Framework Award Form;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Data Protection officer"	has the meaning given to it in the UK GDPR;
Data Subject"	has the meaning given to it in the UK GDPR;
Data Subject access Request"	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;
Deductions"	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under a Call-Off Contract;
Default"	any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority;
Default management charge"	has the meaning given to it in Paragraph 8.1.1 of Framework Schedule 5 (Management Charges and Information);
Delay Payments"	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
Deliverables"	Goods and/or Services that may be ordered under the Contract including the Documentation;
Delivery"	delivery of the relevant Deliverable or Milestone in accordance with the terms of a Call-Off Contract as confirmed and accepted by the Buyer by either (a) confirmation in writing to the Supplier; or (b) where Call-Off Schedule 13 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. " Deliver " and " Delivered " shall be construed accordingly;
Disclosing Party"	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);
Dispute"	any claim, dispute or difference (whether contractual or non-contractual) arising out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;
Dispute resolution procedure"	the dispute resolution procedure set out in Clause 34 (Resolving disputes);
Documentation"	descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as:

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>l) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables</p> <p>m) is required by the Supplier in order to provide the Deliverables; and/or</p> <p>n) has been or shall be generated for the purpose of providing the Deliverables;</p>
DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of Tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions;
DPA 2018"	the Data Protection Act 2018;
Due Diligence Information"	any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date;
Effective Date"	the date on which the final Party has signed the Contract;
EIR"	the Environmental Information Regulations 2004;
Electronic Invoice"	an invoice which has been issued, transmitted and received in a structured electronic format which allows for its automatic and electronic processing and which complies with (a) the European standard and (b) any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870;
Employment Regulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC;
End Date"	<p>the earlier of:</p> <p>a) the Expiry Date (as extended by any Extension Period exercised by the Relevant Authority under Clause 10.1.2); or</p> <p>b) if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract;</p>
Environmental Policy"	to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer;
Equality and Human Rights Commission"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
Estimated Year 1	the anticipated total Charges payable by the Buyer in the first Contract

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Estimated Yearly Charges"	<p>means for the purposes of calculating each Party's annual liability under clause 11.2 :</p> <ul style="list-style-type: none"> i) in the first Contract Year, the Estimated Year 1 Charges; or ii) in the any subsequent Contract Years, the Charges paid or payable in the previous Call-off Contract Year; or iii) after the end of the Call-off Contract, the Charges paid or payable in the last Contract Year during the Call-off Contract Period;
"Exempt Buyer"	<p>a public sector purchaser that is:</p> <ul style="list-style-type: none"> a) eligible to use the Framework Contract; and b) is entering into an Exempt Call-off Contract that is not subject to (as applicable) any of: <ul style="list-style-type: none"> i) the Regulations; ii) the Concession Contracts Regulations 2016 (SI 2016/273); iii) the Utilities Contracts Regulations 2016 (SI 2016/274); iv) the Defence and Security Public Contracts Regulations 2011 (SI 2011/1848); v) the Remedies Directive (2007/66/EC); vi) Directive 2014/23/EU of the European Parliament and Council; vii) Directive 2014/24/EU of the European Parliament and Council; viii) Directive 2014/25/EU of the European Parliament and Council; or ix) Directive 2009/81/EC of the European Parliament and Council;
"Exempt Call-off Contract"	<p>the contract between the Exempt Buyer and the Supplier for Deliverables which consists of the terms set out and referred to in the Order Form incorporating and, where necessary, amending, refining or adding to the terms of the Framework Contract;</p>
"Exempt Procurement Amendments"	<p>any amendments, refinements or additions to any of the terms of the Framework Contract made through the Exempt Call-off Contract to reflect the specific needs of an Exempt Buyer to the extent permitted by and in accordance with any legal requirements applicable to that Exempt Buyer;</p>

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Existing IPR"	any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise);
Exit Day"	shall have the meaning in the European Union (Withdrawal) Act 2018;
Expiry Date"	the Framework Expiry Date or the Call-Off Expiry Date (as the context dictates);
Extension Period"	the Framework Optional Extension Period or the Call-Off Optional Extension Period as the context dictates;
"Financial Reports"	<p>a report by the Supplier to the Buyer that:</p> <ul style="list-style-type: none"> a) provides a true and fair reflection of the Costs and Supplier Profit Margin forecast by the Supplier; b) provides a true and fair reflection of the costs and expenses to be incurred by Key Subcontractors (as requested by the Buyer); c) is in the same software package (Microsoft Excel or Microsoft Word), layout and format as the blank templates which have been issued by the Buyer to the Supplier on or before the Start Date for the purposes of the Contract; and <p>is certified by the Supplier's Chief Financial Officer or Director of Finance;</p>
FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
Force Majeure Event"	<p>any event outside the reasonable control of either Party affecting its performance of its obligations under the Contract arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including:</p> <ul style="list-style-type: none"> a) riots, civil commotion, war or armed conflict; b) acts of terrorism; c) acts of government, local government or regulatory bodies; d) fire, flood, storm or earthquake or other natural disaster, <p>but excluding any industrial dispute relating to the Supplier, the Supplier Staff or any other failure in the Supplier or the Subcontractor's supply chain;</p>
Force Majeure Notice"	a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Framework Award form"	the document outlining the Framework Incorporated Terms and crucial information required for the Framework Contract, to be executed by the Supplier and CCS;
Framework contract"	the framework agreement established between CCS and the Supplier in accordance with Regulation 33 by the Framework Award Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the notice published on the Find a Tender Service;
Framework Contract period"	the period from the Framework Start Date until the End Date of the Framework Contract;
Framework Expiry Date"	the scheduled date of the end of the Framework Contract as stated in the Framework Award Form;
Framework incorporated Terms"	the contractual terms applicable to the Framework Contract specified in the Framework Award Form;
Framework Optional extension Period"	such period or periods beyond which the Framework Contract Period may be extended as specified in the Framework Award Form;
Framework Price(s)"	the price(s) applicable to the provision of the Deliverables set out in Framework Schedule 3 (Framework Prices);
Framework Special terms"	any additional terms and conditions specified in the Framework Award Form incorporated into the Framework Contract;
Framework Start Date"	the date of start of the Framework Contract as stated in the Framework Award Form;
Framework Tender Response"	the tender submitted by the Supplier to CCS and annexed to or referred to in Framework Schedule 2 (Framework Tender);
Further Competition procedure"	the further competition procedure described in Framework Schedule 7 (Call-Off Award Procedure);
UK GDPR"	the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679);
General Anti-Abuse Rule"	a) the legislation in Part 5 of the Finance Act 2013 and; and b) any future legislation introduced into parliament to counteract Tax advantages arising from abusive arrangements to avoid National Insurance contributions;
General Change in Law"	a Change in Law where the change is of a general legislative nature (including Tax or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"Gold Contract"	a Call-Off Contract categorised as a Gold contract using the Cabinet Office Contract Tiering Tool;
Goods"	goods made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form ;
Good Industry practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
Government"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
Government Data"	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 of the Authority's Confidential Information, and which: <ul style="list-style-type: none"> 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 a Contract;
Guarantor"	the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract;
Halifax Abuse principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
"HM Government"	Her Majesty's Government;
HMRC"	Her Majesty's Revenue and Customs;
ICT Policy"	the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;
Impact Assessment"	an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including: <ul style="list-style-type: none"> a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract; b) details of the cost of implementing the proposed Variation; c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Framework Prices/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; d) a timetable for the implementation, together with any proposals for the testing of the Variation; and e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Implementation plan"	the plan for provision of the Deliverables set out in Call-Off Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;
Indemnifier"	a Party from whom an indemnity is sought under this Contract;
Independent control"	where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and "Independent Controller" shall be construed accordingly;
Indexation"	the adjustment of an amount or sum in accordance with Framework Schedule 3 (Framework Prices) and the relevant Order Form;
Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
Information commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
Initial Period"	the initial term of a Contract specified in the Framework Award Form or the Order Form, as the context requires;
Insolvency Event"	<p>with respect to any person, means:</p> <p>(a) that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or:</p> <p>(i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or</p> <p>(ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986;</p> <p>(b) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;</p> <p>(c) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person;</p> <p>(d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person's assets and such attachment or process is not discharged within 14 days;</p>

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>(e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;</p> <p>(f) where that person is a company, a LLP or a partnership:</p> <p>(i) a petition is presented (which is not dismissed within 14 days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;</p> <p>(ii) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at Court or given or if an administrator is appointed, over that person;</p> <p>(iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or</p> <p>(iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or</p> <p>(g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above;</p>
Installation Works"	all works which the Supplier is to carry out at the beginning of the Call-Off Contract Period to install the Goods in accordance with the Call-Off Contract;
Intellectual Property rights" or "IPR"	<p>a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information;</p> <p>b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and</p> <p>c) all other rights having equivalent or similar effect in any country or jurisdiction;</p>
Invoicing Address"	the address to which the Supplier shall invoice the Buyer as specified in the Order Form;
IPR Claim"	any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

IR35"	the off-payroll rules requiring individuals who work through their company pay the same income tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies ;
"ISO"	International Organization for Standardization;
Joint Controller agreement"	the agreement (if any) entered into between the Relevant Authority and the Supplier substantially in the form set out in Annex 2 of Joint Schedule 11 (<i>Processing Data</i>);
Joint Controllers"	where two or more Controllers jointly determine the purposes and means of Processing;
Key Staff"	the individuals (if any) identified as such in the Order Form;
Key Sub-Contract"	each Sub-Contract with a Key Subcontractor;
Key Subcontractor"	any Subcontractor: a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or b) which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or c) with a Sub-Contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under the Call-Off Contract, and the Supplier shall list all such Key Subcontractors in section 19 of the Framework Award Form and in the Key Subcontractor Section in Order Form;
Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date;
Law"	any law, 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, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply;
Losses"	all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and " Loss " shall be interpreted accordingly;
Lots"	the number of lots specified in Framework Schedule 1 (Specification), if applicable;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Management charge"	the sum specified in the Framework Award Form payable by the Supplier to CCS in accordance with Framework Schedule 5 (Management Charges and Information);
Management information" or "MI"	the management information specified in Framework Schedule 5 (Management Charges and Information);
MI Default"	means when two (2) MI Reports are not provided in any rolling six (6) month period
MI Failure"	means when an MI report: <ul style="list-style-type: none"> a) contains any material errors or material omissions or a missing mandatory field; or b) is submitted using an incorrect MI reporting Template; or c) is not submitted by the reporting date (including where a declaration of no business should have been filed);
MI Report"	means a report containing Management Information submitted to the Authority in accordance with Framework Schedule 5 (Management Charges and Information);
MI Reporting template"	means the form of report set out in the Annex to Framework Schedule 5 (Management Charges and Information) setting out the information the Supplier is required to supply to the Authority;
Milestone"	an event or task described in the Implementation Plan;
Milestone Date"	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved;
Month"	a calendar month and " Monthly " shall be interpreted accordingly;
National Insurance"	contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004);
New IPR"	<ul style="list-style-type: none"> a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or b) IPR in or arising as a result of the performance of the Supplier's obligations under a Contract and all updates and amendments to the same; <p>but shall not include the Supplier's Existing IPR;</p>
Occasion of Tax non-Compliance"	<p>where:</p> <ul style="list-style-type: none"> a) any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of: <ul style="list-style-type: none"> i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any Tax rules or legislation in any jurisdiction

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;</p> <p>ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or</p> <p>b) any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for Tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion;</p>
Open Book Data "	<p>complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Call-Off Contract, including details and all assumptions relating to:</p> <p>a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables;</p> <p>b) operating expenditure relating to the provision of the Deliverables including an analysis showing:</p> <p>i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables;</p> <p>ii) staff costs broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each grade;</p> <p>iii) a list of Costs underpinning those rates for each grade, being the agreed rate less the Supplier Profit Margin; and</p> <p>iv) Reimbursable Expenses, if allowed under the Order Form;</p> <p>c) Overheads;</p> <p>d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables;</p> <p>e) the Supplier Profit achieved over the Framework Contract Period and on an annual basis;</p> <p>f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier;</p> <p>g) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and</p> <p>h) the actual Costs profile for each Service Period;</p>

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Order"	means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;
Order Form"	a completed Order Form Template (or equivalent information issued by the Buyer) used to create a Call-Off Contract;
Order Form template"	the template in Framework Schedule 6 (Order Form Template and Call-Off Schedules);
Other Contracting authority"	any actual or potential Buyer under the Framework Contract;
Overhead"	those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs";
Parliament"	takes its natural meaning as interpreted by Law;
Party"	in the context of the Framework Contract, CCS or the Supplier, and in the in the context of a Call-Off Contract the Buyer or the Supplier. "Parties" shall mean both of them where the context permits;
Performance indicators" or "PIs"	the performance measurements and targets in respect of the Supplier's performance of the Framework Contract set out in Framework Schedule 4 (Framework Management);
Personal Data"	has the meaning given to it in the UK GDPR;
Personal Data Breach"	has the meaning given to it in the UK GDPR;
Personnel"	all directors, officers, employees, agents, consultants and suppliers of a Party and/or of any Subcontractor and/or Subprocessor engaged in the performance of its obligations under a Contract;
Prescribed Person"	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies ;
Processing"	has the meaning given to it in the UK GDPR;
Processor"	has the meaning given to it in the UK GDPR;
Progress Meeting"	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;
Progress Meeting frequency"	the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form;
Progress Report"	a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Progress Report frequency"	the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form;
Prohibited Acts"	<p>a) to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to:</p> <ul style="list-style-type: none"> i) induce that person to perform improperly a relevant function or activity; or ii) reward that person for improper performance of a relevant function or activity; <p>b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with each Contract; or</p> <p>c) committing any offence:</p> <ul style="list-style-type: none"> i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or ii) under legislation or common law concerning fraudulent acts; or iii) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or <p>d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;</p>
Protective measures"	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 the such measures adopted by it including those outlined in Framework Schedule 9 (Cyber Essentials Scheme), if applicable, in the case of the Framework Contract or Call-Off Schedule 9 (Security), if applicable, in the case of a Call-Off Contract.
"Rating Agency"	as defined in the Framework Award Form or the Order Form, as the context requires;
"Recall"	a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance;
"Recipient Party"	the Party which receives or obtains directly or indirectly Confidential Information;
"Rectification Plan"	the Supplier's plan (or revised plan) to rectify it's breach using the template in Joint Schedule 10 (Rectification Plan) which shall include:

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>a) full details of the Default that has occurred, including a root cause analysis;</p> <p>b) the actual or anticipated effect of the Default; and</p> <p>c) the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable);</p>
"Rectification Plan process"	the process set out in Clause 10.3.1 to 10.3.4 (Rectification Plan Process);
"Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires);
"Reimbursable expenses"	<p>the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Buyer's expenses policy current from time to time, but not including:</p> <p>a) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and</p> <p>b) subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;</p>
"Relevant Authority"	the Authority which is party to the Contract to which a right or obligation is owed, as the context requires;
"Relevant Authority's Confidential Information"	<p>a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR);</p> <p>b) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority's attention or into the Relevant Authority's possession in connection with a Contract; and</p> <p>information derived from any of the above;</p>
"Relevant Requirements"	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010;
Relevant Tax Authority"	HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established;
Reminder Notice"	a notice sent in accordance with Clause 10.5 given by the Supplier to the Buyer providing notification that payment has not been received on time;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Replacement deliverables"	any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Call-Off Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement subcontractor"	a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor);
"Replacement Supplier"	any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer;
"Request For information"	a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs;
"Required Insurances"	the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form;
"RTI"	Real Time Information;
"Satisfaction Certificate"	the certificate (materially in the form of the document contained in of Part B of Call-Off Schedule 13 (Implementation Plan and Testing) or as agreed by the Parties where Call-Off Schedule 13 is not used in this Contract) granted by the Buyer when the Supplier has met all of the requirements of an Order, Achieved a Milestone or a Test;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to Call-Off Schedule 9 (Security) (if applicable);
"Security Policy"	the Buyer's security policy, referred to in the Order Form, in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;
Self Audit Certificate"	means the certificate in the form as set out in Framework Schedule 8 (Self Audit Certificate);
"Serious Fraud Office"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Service Levels"	any service levels applicable to the provision of the Deliverables under the Call Off Contract (which, where Call Off Schedule 14 (Service Levels) is used in this Contract, are specified in the Annex to Part A of such Schedule);
"Service Period"	has the meaning given to it in the Order Form;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Services"	services made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form;
"Service Transfer"	any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor;
"Service Transfer Date"	the date of a Service Transfer;
"Sites"	any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables;
"SME"	an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium enterprises;
"Special Terms"	any additional Clauses set out in the Framework Award Form or Order Form which shall form part of the respective Contract;
Specific Change in Law"	a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date;
"Specification"	the specification set out in Framework Schedule 1 (Specification), as may, in relation to a Call-Off Contract, be supplemented by the Order Form;
"Standards"	any: a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with; b) standards detailed in the specification in Schedule 1 (Specification); c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time; d) relevant Government codes of practice and guidance applicable from time to time;
"Start Date"	in the case of the Framework Contract, the date specified on the Framework Award Form, and in the case of a Call-Off Contract, the date specified in the Order Form;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Statement of Requirements"	a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Call-Off Procedure;
"Storage Media"	the part of any device that is capable of storing and retrieving data;
"Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than a Call-Off Contract or the Framework Contract, pursuant to which a third party: a) provides the Deliverables (or any part of them); b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	any third Party appointed to process Personal Data on behalf of that Processor related to a Contract;
"Supplier"	the person, firm or company identified in the Framework Award Form;
"Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Call-Off Contract but excluding the Buyer Assets;
Supplier Authorised Representative"	the representative appointed by the Supplier named in the Framework Award Form, or later defined in a Call-Off Contract;
Supplier's Confidential Information"	a) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier; b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier's attention or into the Supplier's possession in connection with a Contract; c) Information derived from any of (a) and (b) above;
"Supplier's Contract Manager"	the person identified in the Order Form appointed by the Supplier to oversee the operation of the Call-Off Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment;
"Supplier Equipment"	the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Call-Off Contract;
Supplier Marketing Contact"	shall be the person identified in the Framework Award Form;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Supplier Non-Performance "	where the Supplier has failed to: a) Achieve a Milestone by its Milestone Date; b) provide the Goods and/or Services in accordance with the Service Levels ; and/or c) comply with an obligation under a Contract;
Supplier Profit"	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions) and total Costs (in nominal cash flow terms) in respect of a Call-Off Contract for the relevant period;
Supplier Profit margin"	in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;
Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;
Supporting documentation"	sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Call-Off Contract detailed in the information are properly payable;
Tax"	a) all forms of taxation whether direct or indirect; b) national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction; c) all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions, levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and d) any penalty, fine, surcharge, interest, charges or costs relating to any of the above, in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction;
Termination Notice"	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate a Contract on a specified date and setting out the grounds for termination;
Test Issue"	any variance or non-conformity of the Deliverables from their requirements as set out in a Call-Off Contract;
Test Plan"	a plan: a) for the Testing of the Deliverables; and b) setting out other agreed criteria related to the achievement of Milestones;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Tests "	any tests required to be carried out pursuant to a Call-Off Contract as set out in the Test Plan or elsewhere in a Call-Off Contract and "Tested" and "Testing" shall be construed accordingly;
Third Party IPR"	Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
Transferring Supplier Employees"	those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;
Transparency information"	the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for – <ul style="list-style-type: none"> (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and (ii) Commercially Sensitive Information;
Transparency reports"	the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Call-Off Schedule 1 (Transparency Reports);
"TUPE"	Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other regulations or UK legislation implementing the Acquired Rights Directive
"United Kingdom"	the country that consists of England, Scotland, Wales, and Northern Ireland
Variation"	any change to a Contract;
Variation Form"	the form set out in Joint Schedule 2 (Variation Form);
Variation Procedure"	the procedure set out in Clause 24 (Changing the contract);
VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
VCSE"	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables;
Working Day"	any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form;

Joint Schedule 1 (Definitions)
Crown Copyright 2018

Work Day"	Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day; and
Work Hours"	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks.

Joint Schedule 2 (Variation Form)
Crown Copyright 2018

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contract Details		
This variation is between:	[delete as applicable: CCS / Buyer] (" CCS " " the Buyer ") And [insert name of Supplier] (" the Supplier ")	
Contract name:	[insert name of contract to be changed] (" the Contract ")	
Contract reference number:	[insert contract reference number]	
Details of Proposed Variation		
Variation initiated by:	[delete as applicable: CCS/Buyer/Supplier]	
Variation number:	[insert variation number]	
Date variation is raised:	[insert date]	
Proposed variation		
Reason for the variation:	[insert reason]	
An Impact Assessment shall be provided within:	[insert number] days	
Impact of Variation		
Likely impact of the proposed variation:	[Supplier to insert assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: <ul style="list-style-type: none"> [CCS/Buyer to insert original Clauses or Paragraphs to be varied and the changed clause] 	
Financial variation:	Original Contract Value:	£ [insert amount]
	Additional cost due to variation:	£ [insert amount]
	New Contract value:	£ [insert amount]

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by [delete as applicable: CCS / Buyer]
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Joint Schedule 2 (Variation Form)
Crown Copyright 2018

Signed by an authorised signatory for and on behalf of the **[delete]** as applicable: CCS / Buyer]

Signature

Date

Name (in Capitals)

Address

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature

Date

Name (in Capitals)

Address

Joint Schedule 2 (Variation Form)
Crown Copyright 2018

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need to have

- 1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("Additional Insurances") and any other insurances as may be required by applicable Law (together the "Insurances"). The Supplier shall ensure that each of the Insurances is effective no later than:
 - 1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
 - 1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.
- 1.2 The Insurances shall be:
 - 1.2.1 maintained in accordance with Good Industry Practice;
 - 1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;
 - 1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
 - 1.2.4 maintained for at least six (6) years after the End Date.
- 1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. How to manage the insurance

- 2.1 Without limiting the other provisions of this Contract, the Supplier shall:
 - 2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;
 - 2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
 - 2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

Joint Schedule 3 (Insurance Requirements)

Crown Copyright 2018

3. What happens if you aren't insured

- 3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.
- 3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. Evidence of insurance you must provide

- 4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. Making sure you are insured to the required amount

- 5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. Cancelled Insurance

- 6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
- 6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

- 7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

Joint Schedule 3 (Insurance Requirements)

Crown Copyright 2018

- 7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.
- 7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

Joint Schedule 3 (Insurance Requirements)

Crown Copyright 2018

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following [standard] insurance cover from the Framework Start Date in accordance with this Schedule:

- 1.1 Professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000) – all Lots.

- 1.2 Public liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000) – all Lots.

- 1.3 Employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000) – all Lots.

- 1.4 Product liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000) – all Lots.

7.5

Joint Schedule 3 (Insurance Requirements)
Crown Copyright 2018

Joint Schedule 4 (Commercially Sensitive Information)

1. What is the Commercially Sensitive Information?

- 1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
- 1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
- 1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality
1	Contract Commence ment	Breakdown of supplier pricing	Throughout the contract term

Joint Schedule 4 (Commercially Sensitive Information)
Crown Copyright 2018

Joint Schedule 5 (Corporate Social Responsibility)

Definitions

In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"First Tier"	the brand company;
"Second Tier"	the final assembly factory linked to the procured product model; and
"Third Tier"	component production factory linked to the procured product model for strategic components, such as CPU, memory, main logic board, display, battery, power supply unit etc.

1. What we expect from our Suppliers

- 1.1 In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government.
(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)
- 1.2 CCS expects its suppliers and subcontractors to meet the standards set out in that Code. In addition, CCS expects its suppliers and subcontractors to comply with the standards set out in this Schedule.
- 1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

2. Equality and Accessibility

- 2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:
 - 2.1.1 eliminate discrimination, harassment or victimisation of any kind; and
 - 2.1.2 advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

3. Modern Slavery, Child Labour and Inhumane Treatment

- 3.1 The Supplier shall fully cooperate with the appointed independent monitoring organisation (which is subject to change at the sole discretion of the Authority) to monitor the rights of workers in electronics supply chains.
- 3.1.1 The current monitoring organisation is: - Electronics Watch a not-for-profit non-governmental organisation incorporated under Dutch law (No. 62721445 in the Dutch Chamber of Commerce Trade Register). Electronics Watch
- 3.2 For any hardware procured through this Framework Agreement RM6098, the Supplier shall disclose in the prescribed format (see Annex 1) details of its First Tier and/or Second Tier and/or Third Tier supply chains (including country and city factory locations). The Authority will provide this information to Electronics Watch to ensure supply chain labour conditions can be assessed.
- 3.3 The Supplier:
- 3.3.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;
 - 3.3.2 shall not require any Supplier Staff or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;
 - 3.3.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.
 - 3.3.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offences anywhere around the world.
 - 3.3.5 shall make reasonable enquiries to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offences anywhere around the world.
 - 3.3.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;
 - 3.3.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;
 - 3.3.8 shall prepare and deliver to CCS, 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 with its annual certification of compliance with Paragraph 3;

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

- 3.3.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;
- 3.3.10 shall not use or allow child or slave labour to be used by its Subcontractors;
- 3.3.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

"Helpline" means the mechanism for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at <https://www.modernslaveryhelpline.org/report> or by telephone on 08000 121 700.

4. Income Security**4.1 The Supplier shall:**

- 4.1.1 ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;
- 4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;
- 4.1.3 not make deductions from wages:
 - (a) as a disciplinary measure
 - (b) except where permitted by law; or
 - (c) without expressed permission of the worker concerned;
- 4.1.4 record all disciplinary measures taken against Supplier Staff; and
- 4.1.5 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

5. Working Hours

5.1 The Supplier shall:

- 5.1.1 ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;
- 5.1.2 that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;
- 5.1.3 ensure that use of overtime used responsibly, taking into account:
 - the extent;
 - frequency; and
 - hours worked;

by individuals and by the Supplier Staff as a whole;

5.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

5.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

- 5.3.1 this is allowed by national law;
- 5.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;
appropriate safeguards are taken to protect the workers' health and safety; and
- 5.3.3 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

5.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

6. Sustainability

6.1 The supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at:

<https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs>

6.2 The Supplier shall use reasonable endeavours to avoid the use of paper and card in carrying out its obligations under this Contract. Where unavoidable under reasonable endeavours, the Supplier shall ensure that any paper or card deployed in the performance of the Services consists of

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

one hundred percent (100%) recycled content and used on both sides where feasible to do so

- 6.3 The Supplier shall complete and provide CCS with a Carbon Reduction Plan.
- 6.4 The Supplier shall progress towards carbon net zero during the lifetime of the framework.

Annex 1

Joint Schedule 5 - Annex 1 Factory Disclosure Form - TePAS2 RM 6098



Joint Schedule 5 -
Annex 1 Factory Discl

Joint Schedule 6 (Key Subcontractors)

1. Restrictions on certain subcontractors

- 1.1 The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.
- 1.2 The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.
- 1.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to section 18 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:
 - 1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
 - 1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
 - 1.3.3 the proposed Key Subcontractor employs unfit persons.
- 1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:
 - 1.4.1 the proposed Key Subcontractor's name, registered office and company registration number;
 - 1.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;
 - 1.4.3 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm's-length" terms;
 - 1.4.4 for CCS, the Key Sub-Contract price expressed as a percentage of the total projected Framework Price over the Framework Contract Period;
 - 1.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and
 - 1.4.6 (where applicable) Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.

Joint Schedule 6 (Key Subcontractors)

Crown Copyright 2018

- 1.5 If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:
 - 1.5.1 a copy of the proposed Key Sub-Contract; and
 - 1.5.2 any further information reasonably requested by CCS and/or the Buyer.
- 1.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:
 - 1.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;
 - 1.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;
 - 1.6.3 a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;
 - 1.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;
 - 1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:
 - (a) the data protection requirements set out in Clause 14 (Data protection);
 - (b) the FOIA and other access request requirements set out in Clause 16 (When you can share information);
 - (c) the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;
 - (d) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and
 - (e) the conduct of audits set out in Clause 6 (Record keeping and reporting);
 - 1.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the Buyer can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and
 - 1.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

Joint Schedule 6 (Key Subcontractors)
Crown Copyright 2018

Joint Schedule 7 (Financial Difficulties)

1. Definitions

1.1 In this Schedule, the following definitions shall apply:

applicable Financial Indicators”	means the financial indicators from Paragraph 5.1 of this Schedule which are to apply to the Monitored Suppliers as set out in Paragraph 5.2 of this Schedule;
Board”	means the Supplier’s board of directors;
Board Confirmation”	means written confirmation from the Board in accordance with Paragraph 8 of this Schedule;
Bronze Contract”	Call-Off Contract categorised as a Bronze contract using the Cabinet Office Contract Tiering Tool;
Cabinet Office Markets and Suppliers Team”	means the UK Government’s team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;
Credit Rating Threshold”	the minimum credit rating level for each entity in the FDE Group as set out in Annex 1 to this Schedule;
DE Group”	means the Supplier,
Financial Distress Event”	copy of the events listed in Paragraph 3.1 of this Schedule;
Financial Distress Remediation Plan”	plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with the Contract in the event that a Financial Distress Event occurs;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

Financial Indicators”	In respect of the Supplier, Key Sub-contractors and the Guarantor, means each of the financial indicators set out at paragraph 5.1 of this Schedule and in respect of each Monitored Supplier, means those Applicable Financial Indicators;
Financial Target Thresholds”	means the target thresholds for each of the Financial Indicators set out at paragraph 5.1 of this Schedule;
Monitored Suppliers”	means those entities specified at paragraph 5.2 of this Schedule;
Rating Agencies”	The rating agencies listed in Annex 1 of this Schedule;
strategic Supplier”	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers .

2. Warranties and duty to notify

2.1 The Supplier warrants and represents to the Relevant Authority for the benefit of the Relevant Authority that as at the Effective Date:

- 2.1.1 the long term credit ratings issued for each entity in the FDE Group by each of the Rating Agencies are as set out in Annex 2 to this Schedule; and
- 2.1.2 the financial position or, as appropriate, the financial performance of each of the Supplier, Guarantor and Key Sub-contractors satisfies the Financial Target Thresholds.

2.2 The Supplier shall promptly notify (or shall procure that its auditors promptly notify) the Relevant Authority in writing if there is any downgrade in the credit rating issued by any Rating Agency for any entity in the FDE Group (and in any event within 5 Working Days of the occurrence of the downgrade).

2.3 The Supplier shall:

- 2.3.1 regularly monitor the credit ratings of each entity in the FDE Group with the Rating Agencies;
- 2.3.2 monitor and report on the Financial Indicators for each entity in the FDE Group against the Financial Target Thresholds at least at the frequency set out for each at Paragraph 5.1 (where specified) and in any event, on a regular basis and no less than once a year within ninety (90) days after the Accounting Reference Date; and
- 2.3.3 promptly notify (or shall procure that its auditors promptly notify) the Relevant Authority in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

Event (and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event).

2.4 For the purposes of determining whether a Financial Distress Event has occurred pursuant to the provisions of Paragraphs 3.1, and for the purposes of determining relief under Paragraph 7.1, the credit rating of an FDE Group entity shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated that entity at or below the applicable Credit Rating Threshold.

2.5 Each report submitted by the Supplier pursuant to paragraph 2.3.2 shall:

- 2.5.1 be a single report with separate sections for each of the FDE Group entities;
- 2.5.2 contain a sufficient level of information to enable the Relevant Authority to verify the calculations that have been made in respect of the Financial Indicators;
- 2.5.3 include key financial and other supporting information (including any accounts data that has been relied on) as separate annexes;
- 2.5.4 be based on the audited accounts for the date or period on which the Financial Indicator is based or, where the Financial Indicator is not linked to an accounting period or an accounting reference date, on unaudited management accounts prepared in accordance with their normal timetable; and
- 2.5.5 include a history of the Financial Indicators reported by the Supplier in graph form to enable the Relevant Authority to easily analyse and assess the trends in financial performance.

3. Financial Distress events

3.1 The following shall be Financial Distress Events:

- 3.1.1 the credit rating of an FDE Group entity dropping below the applicable Credit Rating Threshold;
- 3.1.2 an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;
- 3.1.3 there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;
- 3.1.4 an FDE Group entity committing a material breach of covenant to its lenders;
- 3.1.5 a Key Sub-contractor notifying CCS or the Buyer that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

3.1.6 any of the following:

- (a) commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;
- (b) non-payment by an FDE Group entity of any financial indebtedness;
- (c) any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;
- (d) the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or
- (e) the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;

in each case which the Relevant Authority reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance and delivery of the Deliverables in accordance with the Contract; and

3.1.7 any [one] of the Financial Indicators set out at Paragraph 5 for any of the FDE Group entities failing to meet the required Financial Target Threshold.**4. Consequences of Financial Distress Events**

4.1 Immediately upon notification by the Supplier of a Financial Distress Event (or if the Relevant Authority becomes aware of a Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and the Relevant Authority shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

4.2 In the event of a late or non-payment of a Key Sub-contractor pursuant to Paragraph 3.1.5, the Relevant Authority shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier 10 Working Days to:

4.2.1 rectify such late or non-payment; or

4.2.2 demonstrate to the Relevant Authority's reasonable satisfaction that there is a valid reason for late or non-payment.

4.3 The Supplier shall (and shall procure that any Monitored Supplier, the Guarantor and/or any relevant Key Sub-contractor shall):

4.3.1 at the request of the Relevant Authority, meet the Relevant Authority as soon as reasonably practicable (and in any event within 3 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Relevant Authority may permit and notify to the Supplier in writing) to review the effect of the Financial Distress Event on

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

the continued performance and delivery of the Services in accordance with the Contract; and

4.3.2 where the Relevant Authority reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1 that the Financial Distress Event could impact on the continued performance and delivery of the Deliverables in accordance with the Contract:

- (a) submit to the Relevant Authority for its approval, a draft Financial Distress Remediation Plan as soon as reasonably practicable (and in any event, within 10 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Relevant Authority may permit and notify to the Supplier in writing); and
- (b) to the extent that it is legally permitted to do so and subject to Paragraph 4.8, provide such information relating to the Supplier, any Monitored Supplier, Key Sub-contractors and/or the Guarantor as the Buyer may reasonably require in order to understand the risk to the Deliverables, which may include forecasts in relation to cash flow, orders and profits and details of financial measures being considered to mitigate the impact of the Financial Distress Event.

4.4 The Relevant Authority shall not withhold its approval of a draft Financial Distress Remediation Plan unreasonably. If the Relevant Authority does not approve the draft Financial Distress Remediation Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Remediation Plan, which shall be resubmitted to the Relevant Authority within 5 Working Days of the rejection of the first draft. This process shall be repeated until the Financial Distress Remediation Plan is approved by the Relevant Authority or referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms under Paragraph 4.5.

4.5 If the Relevant Authority considers that the draft Financial Distress Remediation Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not ensure the continued performance of the Supplier's obligations in accordance with the Contract, then it may either agree a further time period for the development and agreement of the Financial Distress Remediation Plan or escalate any issues with the draft Financial Distress Remediation Plan using the Dispute Resolution Procedure in Clause 34 of the Core Terms.

4.6 Following approval of the Financial Distress Remediation Plan by the Relevant Authority, the Supplier shall:

4.6.1 on a regular basis (which shall not be less than fortnightly):

- (a) review and make any updates to the Financial Distress Remediation Plan as the Supplier may deem reasonably necessary and/or as may be reasonably requested by the Relevant Authority, so that the plan

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

- remains adequate, up to date and ensures the continued performance and delivery of the Deliverables in accordance with this Contract; and
- (b) provide a written report to the Relevant Authority setting out its progress against the Financial Distress Remediation Plan, the reasons for any changes made to the Financial Distress Remediation Plan by the Supplier and/or the reasons why the Supplier may have decided not to make any changes;
- 4.6.2 where updates are made to the Financial Distress Remediation Plan in accordance with Paragraph 4.6.1, submit an updated Financial Distress Remediation Plan to the Relevant Authority for its approval, and the provisions of Paragraphs 4.4 and 4.5 shall apply to the review and approval process for the updated Financial Distress Remediation Plan; and
- 4.6.3 comply with the Financial Distress Remediation Plan (including any updated Financial Distress Remediation Plan) and ensure that it achieves the financial and performance requirements set out in the Financial Distress Remediation Plan.
- 4.7 Where the Supplier reasonably believes that the relevant Financial Distress Event under Paragraph 4.1 (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Relevant Authority and the Parties may agree that the Supplier shall be relieved of its obligations under Paragraph 4.6.
- 4.8 The Supplier shall use reasonable endeavours to put in place the necessary measures to ensure that the information specified at paragraph 4.3.2(b) is available when required and on request from the Relevant Authority and within reasonable timescales. Such measures may include:
- 4.8.1 obtaining in advance written authority from Key Sub-contractors, the Guarantor and/or Monitored Suppliers authorising the disclosure of the information to the Buyer and/or entering into confidentiality agreements which permit disclosure;
- 4.8.2 agreeing in advance with the Relevant Authority, Key Sub-contractors, the Guarantor and/or Monitored Suppliers a form of confidentiality agreement to be entered by the relevant parties to enable the disclosure of the information to the Relevant Authority;
- 4.8.3 putting in place any other reasonable arrangements to enable the information to be lawfully disclosed to the Relevant Authority (which may include making price sensitive information available to the Relevant Authority's nominated personnel through confidential arrangements, subject to their consent); and
- 4.8.4 disclosing the information to the fullest extent that it is lawfully entitled to do so, including through the use of redaction,

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

anonymisation and any other techniques to permit disclosure of the information without breaching a duty of confidentiality.

5. Financial Indicators

5.1 Subject to the calculation methodology set out at Annex 3 of this Schedule, the Financial Indicators and the corresponding calculations and thresholds used to determine whether a Financial Distress Event has occurred in respect of those Financial Indicators, shall be as follows:

Lots 1 to 7

Financial Indicator	Calculation¹	Financial Target Threshold:	Monitoring and Reporting Frequency
1 Operating Margin	$\text{Operating Margin} = \frac{\text{Operating Profit}}{\text{Revenue}}$	$> 8\%$	<i>Tested and reported yearly in arrears within 90 days of each accounting reference date based upon figures for the 12 months ending on the relevant accounting reference date.</i>
2 Net Debt to EBITDA Ratio	$\text{Net Debt to EBITDA ratio} = \frac{\text{Net Debt}}{\text{EBITDA}}$	$< 3.5 \text{ times}$	<i>Tested and reported yearly in arrears within 90 days of each accounting reference date based upon EBITDA for the 12 months ending on, and Net Debt at, the relevant accounting reference date.</i>
3 Net Debt + Net Pension Deficit to EBITDA ratio	$\text{Net Debt + Net Pension Deficit to EBITDA Ratio} = \frac{(\text{Net Debt} + \text{Net Pension Deficit})}{\text{EBITDA}}$	$< 5 \text{ times}$	<i>Tested and reported yearly in arrears within 90 days of each accounting reference date based upon EBITDA for the 12 months ending on, and the Net Debt and Net Pension Deficit at, the relevant accounting reference date</i>
4 Net Interest Paid Cover	$\text{Net Interest Paid Cover} = \frac{\text{Earnings Before Interest and Tax}}{\text{Net Interest Paid}}$	$> 3 \text{ times}$	<i>Tested and reported yearly in arrears within 90 days of each accounting reference date based upon figures for the 12 months ending on the</i>

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

			<i>relevant accounting reference date.</i>
5 Acid Ratio	<i>Acid Ratio = (Current Assets – Inventories) / Current Liabilities</i>	<i>> 0.8 times</i>	<i>Tested and reported yearly in arrears within 90 days of each accounting reference date based upon figures at the relevant accounting reference date</i>
6 Net Asset value	<i>Net Asset Value = Net Assets</i>	<i>> £0</i>	<i>Tested and reported yearly in arrears within 90 days of each accounting reference date based upon figures at the relevant accounting reference date</i>
7 Group Exposure Ratio	<i>Group Exposure / Gross Assets</i>	<i>< 50%</i>	<i>Tested and reported yearly in arrears within 90 days of each accounting reference date based upon figures at the relevant accounting reference date</i>

Key: 1 – see Annex 3 to this Schedule which sets out the calculation methodology to be used in the calculation of each financial indicator.

5.2 Monitored Suppliers – NOT USED

--	--

Joint Schedule 7 (Financial Difficulties)
Crown Copyright 2021

	2
	2
	2

6. Termination rights

6.1 The Relevant Authority shall be entitled to terminate the Contract if:

- 6.1.1 the Supplier fails to notify the Relevant Authority of a Financial Distress Event in accordance with Paragraph 2.3.3;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

6.1.2 the Parties fail to agree a Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraphs 4.3 to 4.5; and/or

6.1.3 the Supplier fails to comply with the terms of the Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraph 4.6.3,

which shall be deemed to be an event to which Clause 10.4.1 of the Core Terms applies and Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply accordingly.

7. Primacy of Credit Ratings

7.1 Without prejudice to the Supplier's obligations and the Relevant Authority's rights and remedies under Paragraph 2, if, following the occurrence of a Financial Distress Event pursuant to any of Paragraphs 3.1.2 to 3.1.7, the Rating Agencies review and report subsequently that the credit ratings for the FDE Group entities do not drop below the relevant Credit Rating Thresholds specified for those entities in Annex 2 to this Schedule, then:

7.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and

7.1.2 the Relevant Authority shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

8. Board confirmation

8.1 If the Contract has been specified as a Critical Service Contract under Paragraph 1.1 of Part B of Annex 1 to Call-Off Schedule 8 (Business Continuity and Disaster Recovery) (if applicable) then, subject to Paragraph 8.4 of this Schedule, the Supplier shall within ninety (90) days after each Accounting Reference Date or within 15 months of the previous Board Confirmation (whichever is the earlier) provide a Board Confirmation to the Relevant Authority in the form set out at Annex 4 to this Schedule, confirming that to the best of the Board's knowledge and belief, it is not aware of and has no knowledge:

8.1.1 that a Financial Distress Event has occurred since the later of the Effective Date or the previous Board Confirmation or is subsisting; or

8.1.2 of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event.

8.2 The Supplier shall ensure that in its preparation of the Board Confirmation it exercises due care and diligence and has made reasonable enquiry of all relevant Supplier Staff and other persons as is reasonably necessary to understand and confirm the position.

8.3 In respect of the first Board Confirmation to be provided under this Contract, the Supplier shall provide the Board Confirmation within 15 months of the Effective Date if earlier than the timescale for submission set out in Paragraph 8.1 of this Schedule.

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

8.4 Where the Supplier is unable to provide a Board Confirmation in accordance with Paragraphs 8.1 to 8.3 of this Schedule due to the occurrence of a Financial Distress Event or knowledge of subsisting matters which could reasonably be expected to cause a Financial Distress Event, it will be sufficient for the Supplier to submit in place of the Board Confirmation, a statement from the Board of Directors to the Buyer (and where the Supplier is a Strategic Supplier, the Supplier shall send a copy of the statement to the Cabinet Office Markets and Suppliers Team) setting out full details of any Financial Distress Events that have occurred and/or the matters which could reasonably be expected to cause a Financial Distress Event.

9. Optional Clauses

9.1 Where a Buyer's Call-Off Contract is a Bronze Contract, if specified in the Order Form, the terms at Annex 5 shall apply to the Call-Off Contract in place of the foregoing terms of this Joint Schedule 7.

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

Annex 1: Rating Agencies and their standard Rating System

Rating Agency 1 - Dun & Bradstreet

Joint Schedule 7 (Financial Difficulties)
Crown Copyright 2021

Annex 2: Credit Ratings and Credit Rating Thresholds
Supplier: Softcat Plc

Summary			Currency: GBP
KEY DATA ELEMENTS			
KDE Name	Current Status	Details	
PAYDEX®	[REDACTED]	[REDACTED]	
Failure Score			
Maximum Credit Recommendation			
D&B Rating			
Delinquency Score			
Insolvency Process Indicator			

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

Annex 3: Calculation methodology for Financial Indicators

The Supplier shall ensure that it uses the following general and specific methodologies for calculating the Financial Indicators against the Financial Target Thresholds:

General methodology

- 1 **Terminology:** The terms referred to in this Annex are those used by UK companies in their financial statements. Where the entity is not a UK company, the corresponding items should be used even if the terminology is slightly different (for example a charity would refer to a surplus or deficit rather than a profit or loss).
- 2 **Groups:** Where the entity is the holding company of a group and prepares consolidated financial statements, the consolidated figures should be used.
- 3 **Foreign currency conversion:** Figures denominated in foreign currencies should be converted at the exchange rate in force at the relevant date for which the Financial Indicator is being calculated.
- 4 **Treatment of non-underlying items:** Financial Indicators should be based on the figures in the financial statements before adjusting for non-underlying items.

Specific Methodology

Financial Indicator	Specific Methodology
1 Operating Margin	<p>The elements used to calculate the Operating Margin should be shown on the face of the Income Statement in a standard set of financial statements.</p> <p>Figures for Operating Profit and Revenue should exclude the entity's share of the results of any joint ventures or Associates.</p> <p>Where an entity has an operating loss (i.e. where the operating profit is negative), Operating Profit should be taken to be zero.</p>
2 Net Debt to EBITDA Ratio	<p>"Net Debt" = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents</p> <p>"EBITDA" = Operating profit + Depreciation charge + Amortisation charge</p> <p>The majority of the elements used to calculate the Net Debt to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement and Statement of Cash</p>

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

	<p>Flows in a standard set of financial statements but will otherwise be found in the notes to the financial statements.</p> <p><u><i>Net Debt</i></u>: The elements of Net Debt may be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest bearing liabilities (other than retirement benefit obligations) should be included as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but not non-designated hedges). Borrowings should also include balances owed to other group members.</p> <p>Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing.</p> <p>Cash and cash equivalents should include short-term financial investments shown in current assets.</p> <p>Where Net debt is negative (i.e. an entity has net cash), the relevant Financial Target Threshold should be treated as having been met.</p> <p><u><i>EBITDA</i></u>: Operating profit should be shown on the face of the Income Statement and, for the purposes of calculating this Financial Indicator, should include the entity's share of the results of any joint ventures or Associates. <i>The depreciation and amortisation charges for the period may be found on the face of the Statement of Cash Flows or in a Note to the Accounts. Where EBITDA is negative, the relevant Financial Target Threshold should be treated as not having been met (unless Net Debt is also negative, in which case the relevant Financial Target Threshold should be treated as having been met).</i></p>
<p>3</p> <p>Net Debt + Net Pension Deficit to EBITDA ratio</p>	<p><i>“Net Debt”</i> = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents</p> <p><i>“Net Pension Deficit”</i> = Retirement Benefit Obligations – Retirement Benefit Assets</p> <p><i>“EBITDA”</i> = Operating profit + Depreciation charge + Amortisation charge</p> <p>The majority of the elements used to calculate the Net Debt + Net Pension Deficit to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement and Statement of Cash Flows in a standard set of financial</p>

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

	<p>statements but will otherwise be found in the notes to the financial statements.</p> <p><u><i>Net Debt:</i></u> The elements of Net Debt may be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest bearing liabilities (other than retirement benefit obligations) should be included as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but <i>not</i> non-designated hedges). Borrowings should also include balances owed to other group members.</p> <p>Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing.</p> <p>Cash and cash equivalents should include short-term financial investments shown in current assets.</p> <p><u><i>Net Pension Deficit:</i></u> Retirement Benefit Obligations and Retirement Benefit Assets may be shown on the face of the Balance Sheet or in the notes to the financial statements. They may also be described as pension benefits / obligations, post-employment obligations or other similar terms.</p> <p>Where 'Net Debt + Net Pension Deficit' is negative, the relevant Financial Target Threshold should be treated as having been met.</p> <p><u><i>EBITDA:</i></u> Operating profit should be shown on the face of the Income Statement and, for the purposes of calculating this Financial Indicator, should include the entity's share of the results of any joint ventures or Associates.</p> <p>The depreciation and amortisation charges for the period may be found on the face of the Statement of Cash Flows or in a Note to the Accounts.</p> <p>Where EBITDA is negative, the relevant Financial Target Threshold should be treated as not having been met (unless 'Net Debt + Net Pension Deficit' is also negative, in which case the relevant Financial Target Threshold should be regarded as having been met).</p>
<p>4</p> <p>Net Interest Paid Cover</p>	<p><i>"Earnings Before Interest and Tax"</i> = Operating profit</p> <p><i>"Net Interest Paid"</i> = Interest paid – Interest received</p> <p>Operating profit should be shown on the face of the Income Statement in a standard set of financial statements and, for the purposes of calculating this Financial</p>

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

	<p>Indicator, should include the entity's share of the results of any joint ventures or Associates.</p> <p>Interest received and interest paid should be shown on the face of the Cash Flow statement.</p> <p>Where Net interest paid is negative (i.e. the entity has net interest received), the relevant Financial Target Threshold should be treated as having been met.</p>
5 Acid Ratio	All elements that are used to calculate the Acid Ratio are available on the face of the Balance Sheet in a standard set of financial statements.
6 Net Asset value	Net Assets are shown (but sometimes not labelled) on the face of the Balance Sheet of a standard set of financial statements. Net Assets are sometimes called net worth or 'Shareholders' Funds'. They represent the net assets available to the shareholders. Where an entity has a majority interest in another entity in which there are also minority or non-controlling interests (i.e. where it has a subsidiary partially owned by outside investors), Net Assets should be taken inclusive of minority or non-controlling interests (as if the entity owned 100% of such entity).
7 Group Exposure Ratio	<p><i>"Group Exposure" = Balances owed by Group Undertakings + Contingent liabilities assumed in support of Group Undertakings</i></p> <p><i>"Gross Assets" = Fixed Assets + Current Assets</i></p> <p><u>Group Exposure</u>: Balances owed by (ie receivable from) Group Undertakings are shown within Fixed assets or Current assets either on the face of the Balance Sheet or in the relevant notes to the financial statements. In many cases there may be no such balances, in particular where an entity is not a member of a group or is itself the ultimate holding company of the group.</p> <p>Contingent liabilities assumed in support of Group Undertakings are shown in the Contingent Liabilities note in a standard set of financial statements. They include guarantees and security given in support of the borrowings of other group companies, often as part of group borrowing arrangements. Where the contingent liabilities are capped, the capped figure should be taken as their value. Where no cap or maximum is specified, the relevant Financial Target Threshold should automatically be regarded as not having been met.</p>

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

	<p>In many cases an entity may not have assumed any contingent liabilities in support of Group Undertakings, in particular where an entity is not a member of a group or is itself the ultimate holding company of the group.</p> <p><u>Gross Assets</u>: Both Fixed assets and Current assets are shown on the face of the Balance Sheet.</p>
--	--

Joint Schedule 7 (Financial Difficulties)
Crown Copyright 2021

ANNEX 4: BOARD CONFIRMATION

Supplier Name:

Contract Reference Number:

The Board of Directors acknowledge the requirements set out at paragraph 8 of Joint Schedule 7 (*Financial Distress*) and confirm that the Supplier has exercised due care and diligence and made reasonable enquiry of all relevant Supplier Staff and other persons as is reasonably necessary to enable the Board to prepare this statement.

The Board of Directors confirms, to the best of its knowledge and belief, that as at the date of this Board Confirmation it is not aware of and has no knowledge:

- (a) that a Financial Distress Event has occurred since the later of the previous Board Confirmation and the Effective Date or is subsisting;
or
- (b) of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event

On behalf of the Board of Directors:

Chair
Signed
Date
Director
Signed
Date

ANNEX 5: OPTIONAL CLAUSES FOR BRONZE CONTRACTS

1. Definitions

1.1 In this Annex 5, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Credit Rating Threshold"	1 the minimum credit rating level for the Monitored Company as set out in Appendix 2;
"Financial Distress Event"	<p>2 the occurrence or one or more of the following events:</p> <ul style="list-style-type: none"> a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold; b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects; c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party; d) Monitored Company committing a material breach of covenant to its lenders; e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or f) any of the following: <ul style="list-style-type: none"> i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

	<p>ii) non-payment by the Monitored Company of any financial indebtedness;</p> <p>iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or</p> <p>iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company</p> <p>3 in each case which the Relevant Authority reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Call-Off Contract;</p>
"Financial Distress Service Continuity Plan"	4 a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with [each Call-Off] Contract in the event that a Financial Distress Event occurs;
"Monitored Company"	5 Supplier,
"Rating Agencies"	6 the rating agencies listed in Appendix 1.

2. When this Schedule applies

2.1 The Parties shall comply with the provisions of this Annex 5 in relation to the assessment of the financial standing of the Monitored Companies and the consequences of a change to that financial standing.

2.2 The terms of this Annex 5 shall survive:

2.2.1 under the Framework Contract until the later of (a) the termination or expiry of the Framework Contract or (b) the latest date of termination or expiry of any call-off contract entered into under the Framework Contract (which might be after the date of termination or expiry of the Framework Contract); and

2.2.2 under the Call-Off Contract until the termination or expiry of the Call-Off Contract.

3. What happens when your credit rating changes

3.1 The Supplier warrants and represents to the Relevant Authority that as at the Start Date the long term credit ratings issued for the Monitored Companies by each of the Rating Agencies are as set out in Appendix 2.

3.2 The Supplier shall promptly (and in any event within five (5) Working Days) notify the Relevant Authority in writing if there is any downgrade in the credit rating issued by any Rating Agency for a Monitored Company.

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

- 3.3 If there is any downgrade credit rating issued by any Rating Agency for the Monitored Company the Supplier shall ensure that the Monitored Company's auditors thereafter provide the Relevant Authority within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by the Relevant Authority (such requests not to exceed 4 in any Contract Year) with written calculations of the quick ratio for the Monitored Company as at the end of each Contract Year or such other date as may be requested by the Relevant Authority. For these purposes the "quick ratio" on any date means:

$$\frac{A + B + C}{D}$$

where:

A	is the value at the relevant date of all cash in hand and at the bank of the Monitored Company];
B	is the value of all marketable securities held by the Supplier the Monitored Company determined using closing prices on the Working Day preceding the relevant date;
C	is the value at the relevant date of all account receivables of the Monitored]; and
D	is the value at the relevant date of the current liabilities of the Monitored Company].

- 3.4 The Supplier shall:

- 3.4.1 regularly monitor the credit ratings of each Monitored Company with the Rating Agencies; and
- 3.4.2 promptly notify (or shall procure that its auditors promptly notify) the Relevant Authority in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

- 3.5 For the purposes of determining whether a Financial Distress Event has occurred the credit rating of the Monitored Company shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated the Monitored Company at or below the applicable Credit Rating Threshold.

4. What happens if there is a financial distress event

- 4.1 In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if the Relevant Authority becomes aware of the Financial Distress Event without notification and brings the event to the

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

attention of the Supplier), the Supplier shall have the obligations and the Relevant Authority shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6 of this Annex 5.

4.2 [In the event that a Financial Distress Event arises due to a Key Subcontractor notifying the Relevant Authority that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute then, the Relevant Authority shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:

4.2.1 rectify such late or non-payment; or

4.2.2 demonstrate to the Relevant Authority's reasonable satisfaction that there is a valid reason for late or non-payment.]

4.3 The Supplier shall and shall procure that the other Monitored Companies shall:

4.3.1 at the request of the Relevant Authority meet the Relevant Authority as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) to review the effect of the Financial Distress Event on the continued performance of each Contract and delivery of the Deliverables in accordance each Call-Off Contract; and

4.3.2 where the Relevant Authority reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1) that the Financial Distress Event could impact on the continued performance of each Contract and delivery of the Deliverables in accordance with each Call-Off Contract:

- (a) submit to the Relevant Authority for its Approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within ten (10) Working Days of the initial notification (or awareness) of the Financial Distress Event); and
- (b) provide such financial information relating to the Monitored Company as the Relevant Authority may reasonably require.

4.4 If the Relevant Authority does not (acting reasonably) approve the draft Financial Distress Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to the Relevant Authority within five (5) Working Days of the rejection of the first or subsequent (as the case may be) drafts. This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by the Relevant Authority or referred to the Dispute Resolution Procedure.

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

- 4.5 If the Relevant Authority considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not remedy the relevant Financial Distress Event, then it may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the Dispute Resolution Procedure.
- 4.6 Following Approval of the Financial Distress Service Continuity Plan by the Relevant Authority, the Supplier shall:
- 4.6.1 on a regular basis (which shall not be less than Monthly), review the Financial Distress Service Continuity Plan and assess whether it remains adequate and up to date to ensure the continued performance each Contract and delivery of the Deliverables in accordance with each Call-Off Contract;
 - 4.6.2 where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1, submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 4.5 and 4.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and
 - 4.6.3 comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).
- 4.7 Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Relevant Authority and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.
- 4.8 CCS shall be able to share any information it receives from the Buyer in accordance with this Paragraph with any Buyer who has entered into a Call-Off Contract with the Supplier.

5. When CCS or the Buyer can terminate for financial distress

- 5.1 CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:
- 5.1.1 the Supplier fails to notify the Relevant Authority of a Financial Distress Event in accordance with Paragraph 3.4;
 - 5.1.2 The Relevant Authority and the Supplier fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 4.3 to 4.5; and/or
 - 5.1.3 the Supplier fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraph 4.6.3.

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2021

5.2 If the Contract is terminated in accordance with Paragraph 5.1, Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply as if the Contract had been terminated under Clause 10.4.1.

6. What happens If your credit rating is still good

6.1 Without prejudice to the Supplier's obligations and CCS' and the Buyer's rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:

6.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and

6.1.2 The Relevant Authority shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

APPENDIX 1: RATING AGENCIES

Rating Agency 1 – Dunn and Bradstreet

APPENDIX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

Entity	Credit rating (long term)
[REDACTED]	

Joint Schedule 10 (Rectification Plan)
Crown Copyright 2018

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan		
Details of the Default:	[Guidance: Explain the Default, with clear schedule and clause references as appropriate]	
Deadline for receiving the [Revised] Rectification Plan:	[add date (minimum 10 days from request)]	
Signed by [CCS/Buyer] :		Date:
Supplier [Revised] Rectification Plan		
Cause of the Default	[add cause]	
Anticipated impact assessment:	[add impact]	
Actual effect of Default:	[add effect]	
Steps to be taken to rectification:	Steps	Timescale
	1.	[date]
	2.	[date]
	3.	[date]
	4.	[date]
	[...]	[date]
Timescale for complete Rectification of Default	[X] Working Days	
Steps taken to prevent recurrence of Default	Steps	Timescale
	1.	[date]
	2.	[date]
	3.	[date]
	4.	[date]
	[...]	[date]

Joint Schedule 10 (Rectification Plan)

Crown Copyright 2018

Signed by the Supplier:		Date:	
Review of Rectification Plan [CCS/Buyer]			
Outcome of review	[Plan Accepted] [Plan Rejected] [Revised Plan Requested]		
Reasons for Rejection (if applicable)	[add reasons]		
Signed by [CCS/Buyer]		Date:	

Joint Schedule 11 (Processing Data)

Definitions

1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

**“Processor
Personnel”** all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

- (a) “Controller” in respect of the other Party who is “Processor”;
- (b) “Processor” in respect of the other Party who is “Controller”;
- (c) “Joint Controller” with the other Party;
- (d) “Independent Controller” of the Personal Data where the other Party is also “Controller”,

in respect of certain Personal Data under a Contract and shall specify in Annex 1 (*Processing Personal Data*) which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 (*Processing Personal Data*) by the Controller and may not otherwise be determined by the Processor.
4. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
 - (a) a systematic description of the envisaged Processing and the purpose of the Processing;

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

- (b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
- (a) Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*) and shall not Process the Personal Data for any other purpose, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
 - (b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protection Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take 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;
 - (c) ensure that:
 - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
 - (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 Controller or as otherwise permitted by the Contract; and

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

- (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
 - (d) not transfer, Process, or otherwise make available for Processing, Personal Data outside of the UK unless the prior written consent of the Controller has been obtained (such consent may be withheld or subject to such conditions as the Customer considers fit at the Customer's absolute discretion) and the following conditions are fulfilled:
 - (i) the destination country has been recognised as adequate by the UK Government in accordance with Article 45 UK GDPR or section 74 of the DPA 2018;
 - (ii) Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 DPA 2018) as determined by the Controller;
 - (iii) the Data Subject has enforceable rights and effective legal remedies;
 - (iv) the Processor 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 Controller in meeting its obligations); and
 - (v) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data;

if any of the mechanisms relied on under paragraph 6(d) in respect of any transfers of Personal Data by the Processor at any time ceases to be valid, the Processor shall, if possible, implement an alternative mechanism to ensure compliance with the Data Protection Legislation. If no alternative mechanism is available, the Controller and the Processor shall work together in good faith to determine the appropriate measures to be taken, taking into account any relevant guidance and accepted good industry practice. The Controller reserves the right to require the Processor to cease any affected transfers if no alternative mechanism to ensure compliance with Data Protection Legislation is reasonably available; and
 - (e) at the written direction, and absolute discretion, of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to Processing Personal Data under or in connection with the Contract it:

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
 - (b) receives a request to rectify, block or erase any Personal Data;
 - (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
 - (e) 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
 - (f) becomes aware of a Data Loss Event.
8. The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
9. Taking into account the nature of the Processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
- (a) the Controller with full details and copies of the complaint, communication or request;
 - (b) such assistance as is requested by the Controller to enable the Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (d) assistance as requested by the Controller following any Data Loss Event; and/or
 - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
- (a) the Controller determines that the Processing is not occasional;
 - (b) the Controller 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; or

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

- (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
- 13. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
 - (a) notify the Controller in writing of the intended Subprocessor and Processing that will be undertaken by the Subprocessor;
 - (b) obtain the written consent of the Controller (such consent may be withheld or subject to such conditions as the Controller considers fit at the Controller's absolute discretion);
 - (c) enter into a written legally binding agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor, prior to any Personal Data being transferred to or accessed by the Subprocessor; and
 - (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
- 14. Any Processing by a Subprocessor or transfer of Personal Data to a Subprocessor permitted by the Controller shall not relieve the Processor from any of its liabilities, responsibilities and obligations to the Controller under this Joint Schedule 11, and the Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
- 15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 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 Contract).
- 16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

- 17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 3 to this Joint Schedule 11.

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

Independent Controllers of Personal Data

18. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
19. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
22. The Parties shall only provide Personal Data to each other:
 - (a) to the extent necessary to perform their respective obligations under the Contract;
 - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
 - (c) where it has recorded it in Annex 1 (*Processing Personal Data*).
23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):

- (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
26. Each Party shall promptly notify the other Party upon it becoming aware of any Data Loss Event relating to Personal Data provided by the other Party pursuant to the Contract and shall:
- (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Data Loss Event;
 - (b) implement any measures necessary to restore the security of any compromised Personal Data;
 - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
 - (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
27. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (*Processing Personal Data*).
28. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).
29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an

Joint Schedule 11 (Processing Data)
Crown Copyright 2023

Independent Controller of Personal Data in accordance with paragraphs 18 to 28 of this Joint Schedule 11.

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

- 1.1 The contact details of the Relevant Authority's Data Protection Officer are: [REDACTED]
- 1.2 The contact details of the Supplier's Data Protection Officer are: [REDACTED]
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"> ● Customer name – for administrative purposes in setting up the user in immersive labs and for correspondence purposes. ● Email address – for administrative purposes when contacting the customer and is used to access the platform ● IP Address – The immersive labs platform captures IP address of the users to apply additional security and validation checks <p>The Supplier is Controller and the Relevant Authority is Processor NOT APPLICABLE</p> <p><i>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 3 to paragraph 16 of the following Personal Data:</i></p> <p>The Parties are Joint Controllers NOT APPLICABLE</p> <p><i>The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation and in accordance with paragraph 17 in respect of:</i></p>

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

	<p>The Parties are Independent Controllers of Personal Data NOT APPLICABLE</p> <p><i>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation and in accordance with paragraph 18 in respect of:</i></p> <ul style="list-style-type: none">• <i>Business contact details of Supplier Personnel for which the Supplier is the Controller,</i>• <i>Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller,</i>
Subject matter of the Processing	<p>The information provided by the user to via the NHS England service desk and setup on the Immersive Labs platform is used to track labs that have been attempted and completed. As part of the process, a cumulative score is calculated and displayed on a Leader board that is only visible to other members of the organisation.</p> <p>All the data relating to the user and access to the platform is contained within a database that is hosted by Amazon Web Services.</p> <p>If the user has opted in to receive marketing material this information is also held within the marketing email dataset which is also located within the same geographical location.</p>

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

	The email address and name may be used to deliver non-transactional marketing related e.g. customer feedback
Duration of the Processing	<p>Immersive Labs will retain the user profile data for the duration of the lifetime of the account and in line with the commercial contract.</p> <p>After the account has been terminated the remaining data will be removed from the platform as part of contract termination activities.</p> <p>Under GDPR's right to be forgotten there exists a user-initiated process to request accounts are deleted. This will be done using the current request fulfilment process and Immersive labs will action this upon receipt removing the user's account and all associated data.</p>
Nature and purposes of the Processing	<p>The purpose of the Immersive Labs is to test knowledge and solution gathering that would enable NHS England to better understand the NHS estate's education landscape in terms of cyber and information governance so appropriate control measures can be enforced to reduce the likelihood of exploitation of potential vulnerabilities (people, processes, and technology). Ultimately the Immersive Labs solution supports the Cyber Operations's vision to become a Managed Security Services Provider (MSSP) and deliver better health and care outcomes for patients. The solution essentially complements the wider training offerings that the Cyber Operations offer, as well as develops more specific and tailored training based on user feedback/analytics of consumption.</p> <p>The output of both the Immersive Labs solution would enable the Cyber Operations to better understand the NHS estate's educational landscape. The quantitative data will inform key decisions such as investment and technology strategy to deliver better health and care outcomes to patients.</p>
Type of Personal Data being Processed	<ul style="list-style-type: none"> • Customer name – for administrative purposes in setting up the user in immersive labs and for correspondence purposes. • Email address – for administrative purposes when contacting the customer and is used to access the platform. • IP Address – The immersive labs platform captures IP address of the users to apply additional security and validation checks

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

Categories of Data Subject	<i>NHS Staff</i>
International transfers and legal gateway	<i>n/a</i>
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	This will be done upon contract termination with discussions held on how to best remove the user's account and all associated data from the platform and close the whole of the NHS account.

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

Annex 2 – Security

The technical security requirements set out below provide an indication of the types of security measures that might be considered, in order to protect Personal Data. More, or less, measures may be appropriate depending on the subject matter of the contract, but the overall approach must be proportionate. The technical requirements must also be compliant with legislative and regulatory obligations for content and data, such as UK GDPR. The example technical security requirements set out here are intended to supplement, not replace, security schedules that will detail the total contractual security obligations and requirements that the Processor (i.e. a supplier) will be held to account to deliver under contract. Processors are also required to ensure sufficient 'flow-down' of legislative and regulatory obligations to any third party Sub-processors.

External Certifications e.g. Buyers should ensure that Suppliers hold at least Cyber Essentials certification and ISO 27001:2013 certification if proportionate to the service being procured.

Risk Assessment e.g. Supplier should perform a technical information risk assessment on the service supplied and be able to demonstrate what controls are in place to address those risks.

Security Classification of Information e.g. If the provision of the Services requires the Supplier to Process Authority/Buyer Data which is classified as OFFICIAL, OFFICIAL-SENSITIVE or Personal Data, the Supplier shall implement such additional measures as agreed with the Authority/Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable legislative and regulatory obligations.

End User Devices e.g.

- The Supplier shall ensure that any Authority/Buyer Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority/Buyer except where the Authority/Buyer has given its prior written consent to an alternative arrangement.
- The Supplier shall ensure that any device which is used to Process Authority/Buyer Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security>.

Testing e.g. The Supplier shall at their own cost and expense, procure a CHECK or CREST Certified Supplier to perform an ITHC or Penetration Test prior to any live Authority/Buyer data being transferred into their systems. The ITHC scope must be agreed with the Authority/Buyer to ensure it covers all the relevant parts of the system that processes, stores or hosts Authority/Buyer data.

Networking e.g. The Supplier shall ensure that any Authority/Buyer Data which it causes to be transmitted over any public network (including the Internet, mobile

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

Personnel Security e.g. All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard or equivalent including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. The Supplier maybe required to implement additional security vetting for some roles.

Identity, Authentication and Access Control e.g. The Supplier must operate an appropriate access control regime to ensure that users and administrators of the service are uniquely identified. The Supplier must retain records of access to the physical sites and to the service.

Data Destruction/Deletion e.g. The Supplier must be able to demonstrate they can supply a copy of all data on request or at termination of the service, and must be able to securely erase or destroy all data and media that the Authority/Buyer data has been stored and processed on.

Audit and Protective Monitoring e.g. The Supplier shall collect audit records which relate to security events in delivery of the service or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority/Buyer Data. The retention periods for audit records and event logs must be agreed with the Authority/Buyer and documented.

Location of Authority/Buyer Data e.g. The Supplier shall not, and shall procure that none of its Sub-contractors, process Authority/Buyer Data outside the EEA without the prior written consent of the Authority/Buyer and the Supplier shall not change where it or any of its Sub-contractors process Authority/Buyer Data without the Authority/Buyer's prior written consent which may be subject to conditions.

Vulnerabilities and Corrective Action e.g. Suppliers shall procure and implement security patches to vulnerabilities in accordance with the timescales specified in the NCSC Cloud Security Principle 5.

Suppliers must ensure that all COTS Software and Third Party COTS Software be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support.

Secure Architecture e.g. Suppliers should design the service in accordance with:

- NCSC "[Security Design Principles for Digital Services](#)"

Framework Ref: RM6098

Project Version: v1.0

Model Version: v4.6

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

- NCSC "[Bulk Data Principles](#)"
- NSCS "[Cloud Security Principles](#)"

Joint Schedule 11 (Processing Data)
Crown Copyright 2023

Annex 3 - Joint Controller Agreement NOT APPLICABLE

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 3 (Joint Controller Agreement) in replacement of paragraphs 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 18-28 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the N/A

- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
- (b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- (c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
- (d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and
- (e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the N/A privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Relevant Authority each undertake that they shall:

- (a) report to the other Party every N/A months on:

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

- (i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
- (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
- (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
- (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
- (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
- (e) request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

- (g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
 - (i) are aware of and comply with their duties under this Annex 3 (Joint Controller Agreement) and those in respect of Confidential Information;
 - (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
 - (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
- (h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event 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;
- (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and
- (j) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

3. Data Protection Breach

- 3.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Data Loss Event or circumstances that are likely to give rise to a Data Loss Event, providing the other Party and its advisors with:

Framework Ref: RM6098

Project Version: v1.0

Model Version: v4.6

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Data Loss Event under the Data Protection Legislation; and
- (b) all reasonable assistance, including:
 - (i) co-operation with the other Party and the Information Commissioner investigating the Data Loss Event and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
 - (ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Data Loss Event;
 - (iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Data Loss Event; and/or
 - (iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Data Loss Event, with complete information relating to the Data Loss Event, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Data Loss Event as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Data Loss Event, including providing the other Party, as soon as possible and within 48 hours of the Data Loss Event relating to the Data Loss Event, in particular:

- (a) the nature of the Data Loss Event;
- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Data Loss Event; and
- (f) describe the likely consequences of the Data Loss Event.

4. Audit

4.1 The Supplier shall permit:

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

- (a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 3 and the Data Protection Legislation; and/or
- (b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

- (a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and
- (b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

- 7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Data Loss Event ("**Financial Penalties**") then the following shall occur:
- (a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Data Loss Event, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Data Loss Event. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Data Loss Event;
 - (b) if in the view of the Information Commissioner, the Supplier is responsible for the Data Loss Event, in that it is not a Data Loss Event that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Data Loss Event; or
 - (c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Data Loss Event and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Data Loss Event can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).
- 7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Data Loss Event, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Data Loss Event shall be liable for the losses arising from such Data Loss Event. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.
- 7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Data Loss Event (the "Claim Losses"):
- (a) if the Relevant Authority is responsible for the relevant Data Loss Event, then the Relevant Authority shall be responsible for the Claim Losses;

Joint Schedule 11 (Processing Data)

Crown Copyright 2023

- (b) if the Supplier is responsible for the relevant Data Loss Event, then the Supplier shall be responsible for the Claim Losses: and
- (c) if responsibility for the relevant Data Loss Event is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Data Loss Event, having regard to all the circumstances of the Data Loss Event and the legal and financial obligations of the Relevant Authority.

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 3 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

- (a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
- (b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Call-Off Schedule 5 (Pricing Details)
Call-Off Ref:
Crown Copyright 2018

Call-Off Schedule 5 (Pricing Details)

Total Cost (excluding VAT)				
Product / Service	Number	Description		Total
Cyber Professional Licences	Enterprise-wide license	2000+ world leading Cyber Security on demand labs with the catalogue growing weekly Includes a Customer Success Manager who will support with everyday tasks such as licencing and basic reporting		£2,058,473.00
App Sec Cloud Sec	Enterprise-wide license	The aim is to leverage data insights to strengthen the software development life cycle and reduce vulnerabilities in applications		
Crisis Simulation Tool	Enterprise-wide license	Access to a library of cyber incident response scenarios and ability to custom build own scenarios relevant to work area. Catalogue of scenarios is continuously added to		
Screening	Enterprise-wide license	Allows managers to effectively tailor job advertisements to specific technical roles and then test candidates' technical ability before interview. For internal or external candidates		
Team Sim	10 Credits	Prove the effectiveness of Red and Blue Teams as they progress through complex technical scenarios.		
Cyber Workforce Advisor	1 Full Time Dedicated	Full time resource attached to account to drive engagement and ensure successful outcomes. Employed by Immersive Labs, but very much embedded into the NHS		
Total Cost				£ 2,058,473.00

Call-Off Schedule 5 (Pricing Details)
Call-Off Ref:
Crown Copyright 2018

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

Call-Off Schedule 6 (ICT Services)

1. Definitions

- 1.1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Buyer Property"	the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract;
"Buyer Software"	any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;
"Buyer System"	the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
"Commercial off the shelf Software" or "COTS Software"	Non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms
"Core Network"	the provision of any shared central core network capability forming part of the overall Services delivered to the Buyer, which is not specific or exclusive to a specific Call-Off Contract, and excludes any configuration information specifically associated with a specific Call-Off Contract;
"Defect"	any of the following: <ul style="list-style-type: none">a) any error, damage or defect in the manufacturing of a Deliverable; orb) any error or failure of code within the Software which causes a Deliverable to

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

malfunction or to produce unintelligible or incorrect results; or

- c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or
- d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;

"Emergency Maintenance"

ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;

"ICT Environment"

the Buyer System and the Supplier System;

"Licensed Software"

all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;

"Maintenance Schedule"

has the meaning given to it in paragraph 8 of this Schedule;

"Malicious Software"

any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

	software is introduced wilfully, negligently or without knowledge of its existence;
"New Release"	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
"Open Source Software"	computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;
"Operating Environment"	means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: <ul style="list-style-type: none"> a) the Deliverables are (or are to be) provided; or b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or c) where any part of the Supplier System is situated;
"Permitted Maintenance"	has the meaning given to it in paragraph 8.2 of this Schedule;
"Quality Plans"	has the meaning given to it in paragraph 6.1 of this Schedule;
"Sites"	has the meaning given to it in Joint Schedule 1 (Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;
"Software"	Specially Written Software COTS Software and non-COTS Supplier and third party Software;
"Software Supporting Materials"	has the meaning given to it in paragraph 9.1 of this Schedule;

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

"Source Code"

computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;

"Specially Written Software"

any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;

"Supplier System"

the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

- 2.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT Services which are part of the Deliverables.

3. Buyer due diligence requirements

- 3.1. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;
- 3.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;
 - 3.1.2. operating processes and procedures and the working methods of the Buyer;

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- 3.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and
 - 3.1.4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.
- 3.2. The Supplier confirms that it has advised the Buyer in writing of:
- 3.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;
 - 3.2.2. the actions needed to remedy each such unsuitable aspect; and
 - 3.2.3. a timetable for and the costs of those actions.

4. Licensed software warranty

- 4.1. The Supplier represents and warrants that:
- 4.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the Buyer which are necessary for the performance of the Supplier's obligations under this Contract including the receipt of the Deliverables by the Buyer;
 - 4.1.2. all components of the Specially Written Software shall:
 - 4.1.2.1. be free from material design and programming errors;
 - 4.1.2.2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels) and Documentation; and
 - 4.1.2.3. not infringe any IPR.

5. Provision of ICT Services

- 5.1. The Supplier shall:
- 5.1.1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- 5.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;
- 5.1.3. ensure that the Supplier System will be free of all encumbrances;
- 5.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;
- 5.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

6. Standards and Quality Requirements

- 6.1. The Supplier shall develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**").
- 6.2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.
- 6.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.
- 6.4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:
 - 6.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;
 - 6.4.2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and
 - 6.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

7. ICT Audit

- 7.1. The Supplier shall allow any auditor access to the Supplier premises to:
 - 7.1.1. inspect the ICT Environment and the wider service delivery environment (or any part of them);

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- 7.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;
- 7.1.3. review the Supplier's quality management systems including all relevant Quality Plans.

8. Maintenance of the ICT Environment

- 8.1. If specified by the Buyer in the Order Form, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.
- 8.2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (other than to the Core Network) (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.
- 8.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance, including to the Core Network.
- 8.4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

9. Intellectual Property Rights in ICT**9.1. Assignments granted by the Supplier: Specially Written Software**

- 9.1.1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:
 - 9.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and
 - 9.1.1.2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

9.1.2. The Supplier shall:

- 9.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;
- 9.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and
- 9.1.2.3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

- 9.1.3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

9.2. Licences for non-COTS IPR from the Supplier and third parties to the Buyer

- 9.2.1. Unless the Buyer gives its Approval the Supplier must not use any:
 - a) of its own Existing IPR that is not COTS Software;
 - b) third party software that is not COTS Software
- 9.2.2. Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grants to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Central Government Body, any other Central Government Body's) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution,

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

storage, transmission or display) for the Call Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

- 9.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

9.2.3.1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and

9.2.3.2. only use such third party IPR as referred to at paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

- 9.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

- 9.2.5. The Supplier may terminate a licence granted under paragraph 9.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

9.3. Licenses for COTS Software by the Supplier and third parties to the Buyer

- 9.3.1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

- 9.3.2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

- 9.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licensee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

9.3.4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:

9.3.4.1. will no longer be maintained or supported by the developer;
or

9.3.4.2. will no longer be made commercially available

9.4. Buyer's right to assign/novate licences

9.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 9.2 (to:

9.4.1.1. a Central Government Body; or

9.4.1.2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.

9.4.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 9.2.

9.5. Licence granted by the Buyer

9.5.1. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).

9.6. Open Source Publication

9.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

9.6.1.1. suitable for publication by the Buyer as Open Source; and

9.6.1.2. based on Open Standards (where applicable),

and the Buyer may, at its sole discretion, publish the same as Open Source.

9.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:

9.6.2.1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation,

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

running or security of the Specially Written Software, New IPRs or the Buyer System;

- 9.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;
 - 9.6.2.3. do not contain any material which would bring the Buyer into disrepute;
 - 9.6.2.4. can be published as Open Source without breaching the rights of any third party;
 - 9.6.2.5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and
 - 9.6.2.6. do not contain any Malicious Software.
- 9.6.3. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:
- 9.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and
 - 9.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

9.7. Malicious Software

- 9.7.1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.
- 9.7.2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

- 9.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.7.2 shall be borne by the Parties as follows:
- 9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and
 - 9.7.3.2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

10. Supplier-Furnished Terms**10.1. Software Licence Terms**

- 10.1.1. Terms for licensing of non-COTS third party software in accordance with Paragraph 9.2.3 are detailed in Annex A of this Call Off Schedule 6.
- 10.1.2. Terms for licensing of COTS software in accordance with Paragraph 9.3 are detailed in Annex B of this Call Off Schedule 6.

10.2. Software Support & Maintenance Terms

- 10.2.1. Additional terms for provision of Software Support & Maintenance Services are detailed in Annex C of this Call Off Schedule 6.

10.3. Software as a Service Terms

- 10.3.1. Additional terms for provision of a Software as a Service solution are detailed in Annex D of this Call Off Schedule 6.

10.4. As a Service Terms

- 10.4.1. Additional terms for provision of a devices, utility and consumption models for technology infrastructure generally described as "As a Service" solutions are detailed in Annex E to this Call-Off Schedule 6.

11. Customer Premises**11.1. Licence to occupy Customer Premises**

- 11.1.1. Any Customer Premises shall be made available to the Supplier on a non-exclusive licence basis free of charge and shall be used by the Supplier solely for the purpose of performing its obligations under this

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

Call- Off Contract. The Supplier shall have the use of such Customer Premises as licensee and shall vacate the same immediately upon completion, termination, expiry or abandonment of this Call-Off Contract and in accordance with Call-Off Schedule 10 (Exit Management).

- 11.1.2. The Supplier shall limit access to the Buyer Premises to such Supplier Staff as is necessary to enable it to perform its obligations under this Call-Off Contract and the Supplier shall co-operate (and ensure that the Supplier Staff co-operate) with such other persons working concurrently on such Buyer Premises as the Buyer may reasonably request.
- 11.1.3. Save in relation to such actions identified by the Supplier in accordance with paragraph 3.2 of this Call-Off Schedule 6 and set out in the Order Form (or elsewhere in this Call Off Contract), should the Supplier require modifications to the Buyer Premises, such modifications shall be subject to Approval and shall be carried out by the Buyer at the Supplier's expense. The Buyer shall undertake any modification work which it approves pursuant to this paragraph 11.1.3 without undue delay. Ownership of such modifications shall rest with the Buyer.
- 11.1.4. The Supplier shall observe and comply with such rules and regulations as may be in force at any time for the use of such Buyer Premises and conduct of personnel at the Buyer Premises as determined by the Buyer, and the Supplier shall pay for the full cost of making good any damage caused by the Supplier Staff other than fair wear and tear. For the avoidance of doubt, damage includes without limitation damage to the fabric of the buildings, plant, fixed equipment or fittings therein.
- 11.1.5. The Parties agree that there is no intention on the part of the Buyer to create a tenancy of any nature whatsoever in favour of the Supplier or the Supplier Staff and that no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to this Call-Off Contract, the Buyer retains the right at any time to use any Buyer Premises in any manner it sees fit.

11.2. Security of Buyer Premises

- 11.2.1. The Buyer shall be responsible for maintaining the security of the Buyer Premises. The Supplier shall comply with the reasonable security requirements of the Buyer while on the Buyer Premises.
- 11.2.2. The Buyer shall afford the Supplier upon Approval (the decision to Approve or not will not be unreasonably withheld or delayed) an opportunity to inspect its physical security arrangements.

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

12. Buyer Property

- 12.1.** Where the Buyer issues Buyer Property free of charge to the Supplier such Buyer Property shall be and remain the property of the Buyer and the Supplier irrevocably licences the Buyer and its agents to enter upon any premises of the Supplier during normal business hours on reasonable notice to recover any such Buyer Property.
- 12.2.** The Supplier shall not in any circumstances have a lien or any other interest on the Buyer Property and at all times the Supplier shall possess the Buyer Property as fiduciary agent and bailee of the Buyer.
- 12.3.** The Supplier shall take all reasonable steps to ensure that the title of the Buyer to the Buyer Property and the exclusion of any such lien or other interest are brought to the notice of all Sub-Contractors and other appropriate persons and shall, at the Buyer's request, store the Buyer Property separately and securely and ensure that it is clearly identifiable as belonging to the Buyer.
- 12.4.** The Buyer Property shall be deemed to be in good condition when received by or on behalf of the Supplier unless the Supplier notifies the Buyer otherwise within five (5) Working Days of receipt.
- 12.5.** The Supplier shall maintain the Buyer Property in good order and condition (excluding fair wear and tear) and shall use the Buyer Property solely in connection with this Call-Off Contract and for no other purpose without Approval.
- 12.6.** The Supplier shall ensure the security of all the Buyer Property whilst in its possession, either on the Sites or elsewhere during the supply of the Services, in accordance with Call- Off Schedule 9 (Security) and the Buyer's reasonable security requirements from time to time.
- 12.7.** The Supplier shall be liable for all loss of, or damage to the Buyer Property, (excluding fair wear and tear), unless such loss or damage was solely caused by a Buyer Cause. The Supplier shall inform the Buyer immediately of becoming aware of any defects appearing in or losses or damage occurring to the Buyer Property.

13. Supplier Equipment

- 13.1.** Unless otherwise stated in this Call Off Contract, the Supplier shall provide all the Supplier Equipment necessary for the provision of the Services.
- 13.2.** The Supplier shall not deliver any Supplier Equipment nor begin any work on the Buyer Premises without obtaining Approval.

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

13.3. The Supplier shall be solely responsible for the cost of carriage of the Supplier Equipment to the Sites and/or any Buyer Premises, including its off-loading, removal of all packaging and all other associated costs. Likewise on the Call-Off Expiry Date the Supplier shall be responsible for the removal of all relevant Supplier Equipment from the Sites and/or any Buyer Premises, including the cost of packing, carriage and making good the Sites and/or the Buyer Premises following removal.

13.4. All the Supplier's property, including Supplier Equipment, shall remain at the sole risk and responsibility of the Supplier, except that the Buyer shall be liable for loss of or damage to any of the Supplier's property located on Buyer Premises which is due to the negligent act or omission of the Buyer.

13.5. 4.5 Subject to any express provision of the BCDR Plan (if applicable) to the contrary, the loss or destruction for any reason of any Supplier Equipment shall not relieve the Supplier of its obligation to supply the Services in accordance with this Call Off Contract, including the Service Levels.

13.6. The Supplier shall maintain all Supplier Equipment within the Sites and/or the Buyer Premises in a safe, serviceable and clean condition.

13.7. The Supplier shall, at the Buyer's written request, at its own expense and as soon as reasonably practicable:

13.7.1. remove from the Buyer Premises any Supplier Equipment or any component part of Supplier Equipment which in the reasonable opinion of the Buyer is either hazardous, noxious or not in accordance with this Call-Off Contract; and

13.7.2. replace such Supplier Equipment or component part of Supplier Equipment with a suitable substitute item of Supplier Equipment.

Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

ANNEX A

Non-COTS Third Party Software Licensing Terms

ANNEX B

Unlimited cyber enterprise license that will allow health and care users access to the 2000+ labs and future growth of the catalogue, this includes but not limited to:

- **Application and Cloud security**
- **Crisis simulation tool**
- **Screening**
- **Team Sim**
- **Cyber workforce advisor**

COTS Licensing Terms

ANNEX C

Software Support & Maintenance Terms

Immersive Labs provides support for both the web application and underlying content served in the platform. An online support function maintained through the following email address: support@immersivelabs.com. Working hours are 09.00 to 17.30 GMT/BST/EST Monday to Friday (excluding UK bank and US public holidays) (as applicable).

The Immersive Labs Platform is designed to be available 24 hours a day, 7 days a week, 365 days a year. Immersive Labs uses reasonable commercial endeavours to operate a target minimum service availability of 99.5% uptime. We monitor the uptime of our services using a third-party company that generates alerts in the event the site is unavailable. We use a third-party monitoring tool (Uptime Robot) to generate reports, alerts, and dashboards for the uptime of the application

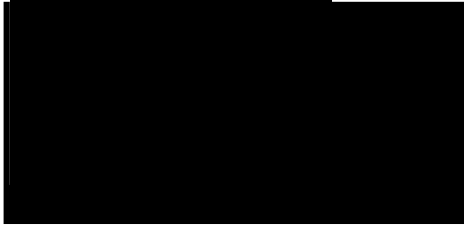
Call-Off Schedule 6 (ICT Services)

Call-Off Ref:

Crown Copyright 2018

ANNEX D

Software as a Service Terms



Annex E

As a Service Terms

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

1. Definitions

- 1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Annual Revenue"	means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology: figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date;
"Appropriate Authority" or "Appropriate Authorities"	means the Buyer and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;
"Associates"	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles;
"BCDR Plan"	has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	has the meaning given to it in Paragraph 2.3.2 of this Schedule;

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

“Class 1 Transaction”	has the meaning set out in the listing rules issued by the UK Listing Authority;
“Control”	the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;
“Corporate Change Event”	<p>means:</p> <ul style="list-style-type: none"> (a) any change of Control of the Supplier or a Parent Undertaking of the Supplier; (b) any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Deliverables; (c) any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Deliverables; (d) a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc; (e) an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier; (f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period; (g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group; (h) any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise,

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

	<p>composition, arrangement or agreement being made with creditors of any member of the Supplier Group;</p> <p>(i) the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or</p> <p>(j) any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales;</p>
“Critical National Infrastructure”	<p>means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:</p> <p>major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or</p> <p>significant impact on the national security, national defence, or the functioning of the UK;</p>
“Critical Service Contract”	<p>a service contract which the Buyer has categorised as a Gold Contract using the Cabinet Office Contract Tiering Tool or which the Buyer otherwise considers should be classed as a Critical Service Contract;</p>
“CRP Information”	<p>means, together, the:</p> <p>Group Structure Information and Resolution Commentary; and</p> <p>UK Public Sector and CNI Contract Information;</p>
“Dependent Parent Undertaking”	<p>means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading,</p>

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

	managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into the Contract, including for the avoidance of doubt the provision of the Deliverables in accordance with the terms of the Contract;
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable);
"Disaster Recovery Deliverables"	the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Group Structure Information and Resolution Commentary"	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 to 4 and Appendix 1 to Part B;
"Parent Undertaking"	has the meaning set out in section 1162 of the Companies Act 2006;
"Public Sector Dependent Supplier"	means a supplier where that supplier, or that supplier's group has Annual Revenue of £50 million or more of which over 50% is generated from UK Public Sector Business;
"Related Supplier"	any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	has the meaning given to it in Paragraph 6.3 of this Schedule;
"Strategic Supplier"	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers ;

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

“Subsidiary Undertaking”	has the meaning set out in section 1162 of the Companies Act 2006;
“Supplier Group”	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
"Supplier's Proposals"	has the meaning given to it in Paragraph 6.3 of this Schedule;
“UK Public Sector Business”	means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations; and
“UK Public Sector / CNI Contract Information”	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 to 4 and Appendix 2 of Part B;

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

Part A: BCDR Plan**1. BCDR Plan**

- 1.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.
- 1.2 At least ninety (90) Working Days prior to the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a "**BCDR Plan**"), which shall detail the processes and arrangements that the Supplier shall follow to:
 - 1.2.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and
 - 1.2.2 the recovery of the Deliverables in the event of a Disaster
- 1.3 The BCDR Plan shall be divided into four sections:
 - 1.3.1 Section 1 which shall set out general principles applicable to the BCDR Plan;
 - 1.3.2 Section 2 which shall relate to business continuity (the "**Business Continuity Plan**");
 - 1.3.3 Section 3 which shall relate to disaster recovery (the "**Disaster Recovery Plan**"); and
 - 1.3.4 Section 4 which shall relate to an Insolvency Event of the Supplier, and Key-Subcontractors and/or any Supplier Group member (the "**Insolvency Continuity Plan**").
- 1.4 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

2. General Principles of the BCDR Plan (Section 1)

- 2.1 Section 1 of the BCDR Plan shall:
 - 2.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;
 - 2.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;
 - 2.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

- 2.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;
- 2.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;
- 2.1.6 contain a risk analysis, including:
 - (a) failure or disruption scenarios and assessments of likely frequency of occurrence;
 - (b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;
 - (c) identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and
 - (d) a business impact analysis of different anticipated failures or disruptions;
- 2.1.7 provide for documentation of processes, including business processes, and procedures;
- 2.1.8 set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;
- 2.1.9 identify the procedures for reverting to "normal service";
- 2.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;
- 2.1.11 identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan;
- 2.1.12 provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans;
- 2.1.13 set out how the business continuity and disaster recovery elements of the BCDR Plan link to the Insolvency Continuity Plan, and how the Insolvency Continuity Plan links to the business continuity and disaster recovery elements of the BCDR Plan;
- 2.1.14 contain an obligation upon the Supplier to liaise with the Buyer and (at the Buyer's request) any Related Supplier with respect to issues concerning insolvency continuity where applicable; and
- 2.1.15 detail how the BCDR Plan links and interoperates with any overarching and/or connected insolvency continuity plan of the Buyer and any of its other Related Suppliers in each case as notified to the Supplier by the Buyer from time to time.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

- 2.2 The BCDR Plan shall be designed so as to ensure that:
- 2.2.1 the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;
 - 2.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;
 - 2.2.3 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and
 - 2.2.4 it details a process for the management of disaster recovery testing.
- 2.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.
- 2.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI's) or Service levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

3. Business Continuity (Section 2)

- 3.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:
- 3.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and
 - 3.1.2 the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.
- 3.2 The Business Continuity Plan shall:
- 3.2.1 address the various possible levels of failures of or disruptions to the provision of Deliverables;
 - 3.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;
 - 3.2.3 specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and
 - 3.2.4 set out the circumstances in which the Business Continuity Plan is invoked.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

4. Disaster Recovery (Section 3)

- 4.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
- 4.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:
- 4.2.1 loss of access to the Buyer Premises;
 - 4.2.2 loss of utilities to the Buyer Premises;
 - 4.2.3 loss of the Supplier's helpdesk or CAFM system;
 - 4.2.4 loss of a Subcontractor;
 - 4.2.5 emergency notification and escalation process;
 - 4.2.6 contact lists;
 - 4.2.7 staff training and awareness;
 - 4.2.8 BCDR Plan testing;
 - 4.2.9 post implementation review process;
 - 4.2.10 any applicable Performance Indicators (PI's) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;
 - 4.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;
 - 4.2.12 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and
 - 4.2.13 testing and management arrangements.

5. Insolvency Continuity Plan (Section 4)

- 5.1 The Insolvency Continuity Plan shall be designed by the Supplier to permit continuity of the business operations of the Buyer supported by the Deliverables through continued provision of the Deliverables following an Insolvency Event of the Supplier, any Key Sub-contractor and/or any Supplier Group member with, as far as reasonably possible, minimal adverse impact.
- 5.2 The Insolvency Continuity Plan shall include the following:
- 5.2.1 communication strategies which are designed to minimise the potential disruption to the provision of the Deliverables, including key contact details in respect of the supply chain and key contact details for

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

operational and contract Supplier Staff, Key Subcontractor personnel and Supplier Group member personnel;

- 5.2.2 identification, explanation, assessment and an impact analysis of risks in respect of dependencies between the Supplier, Key Subcontractors and Supplier Group members where failure of those dependencies could reasonably have an adverse impact on the Deliverables;
- 5.2.3 plans to manage and mitigate identified risks;
- 5.2.4 details of the roles and responsibilities of the Supplier, Key Subcontractors and/or Supplier Group members to minimise and mitigate the effects of an Insolvency Event of such persons on the Deliverables;
- 5.2.5 details of the recovery team to be put in place by the Supplier (which may include representatives of the Supplier, Key Subcontractors and Supplier Group members); and
- 5.2.6 sufficient detail to enable an appointed insolvency practitioner to invoke the plan in the event of an Insolvency Event of the Supplier.

6. Review and changing the BCDR Plan**6.1 The Supplier shall review the BCDR Plan:**

- 6.1.1 on a regular basis and as a minimum once every six (6) Months;
- 6.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 8; and
- 6.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.

6.2 Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.**6.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a "Review**

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

Report") setting out the Supplier's proposals (the "**Supplier's Proposals**") for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

- 6.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
- 6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

7. Testing the BCDR Plan

- 7.1 The Supplier shall test the BCDR Plan:
- 7.1.1 regularly and in any event not less than once in every Contract Year;
 - 7.1.2 in the event of any major reconfiguration of the Deliverables
 - 7.1.3 at any time where the Buyer considers it necessary (acting in its sole discretion).
- 7.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.
- 7.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.
- 7.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.
- 7.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:
- 7.5.1 the outcome of the test;
 - 7.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and
 - 7.5.3 the Supplier's proposals for remedying any such failures.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

- 7.6 Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

8. Invoking the BCDR Plan

- 8.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.
- 8.2 The Insolvency Continuity Plan element of the BCDR Plan, including any linked elements in other parts of the BCDR Plan, shall be invoked by the Supplier:
- 8.2.1 where an Insolvency Event of a Key Sub-contractor and/or Supplier Group member (other than the Supplier) could reasonably be expected to adversely affect delivery of the Deliverables; and/or
 - 8.2.2 where there is an Insolvency Event of the Supplier and the insolvency arrangements enable the Supplier to invoke the plan.

9. Circumstances beyond your control

- 9.1 The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.

10. Amendments to this Schedule in respect of Bronze Contracts

- 10.1 Where a Buyer's Call-Off Contract is a Bronze Contract, if specified in the Order Form, the following provisions of this Call-Off Schedule 8, shall be disapplied in respect of that Contract:
- 10.1.1 Paragraph 1.3.4 of Part A so that the BCDR plan shall only be required to be split into the three sections detailed in paragraphs 1.3.1 to 1.3.3 inclusive;
 - 10.1.2 Paragraphs 2.1.13 to 2.1.15 of Part A, inclusive;
 - 10.1.3 Paragraph 5 (Insolvency Continuity Plan) of Part A;
 - 10.1.4 Paragraph 8.2 of Part A; and
 - 10.1.5 The entirety of Part B of this Schedule.
- 10.2 Where a Buyer's Call-Off Contract is a Bronze Contract, if specified in the Order Form, the following definitions in Paragraph 1 of this Call-Off Schedule 8, shall be deemed to be deleted:
- 10.2.1 Annual Review;
 - 10.2.2 Appropriate Authority or Appropriate Authorities;
 - 10.2.3 Associates;

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

- 10.2.4 Class 1 Transaction;
- 10.2.5 Control;
- 10.2.6 Corporate Change Event;
- 10.2.7 Critical National Infrastructure;
- 10.2.8 Critical Service Contract;
- 10.2.9 CRP Information;
- 10.2.10 Dependent Parent Undertaking;
- 10.2.11 Group Structure Information and Resolution Commentary;
- 10.2.12 Parent Undertaking;
- 10.2.13 Public Sector Dependent Supplier;
- 10.2.14 Subsidiary Undertaking;
- 10.2.15 Supplier Group;
- 10.2.16 UK Public Sector Business; and
- 10.2.17 UK Public Sector/CNI Contract Information.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

Part B: Corporate Resolution Planning**1. Service Status and Supplier Status**

- 1.1 This Contract is not a Critical Service Contract.
- 1.2 The Supplier shall notify the Buyer in writing within 5 Working Days of the Effective Date and throughout the Call-Off Contract Period within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier.

2. Provision of Corporate Resolution Planning Information

- 2.1 Paragraphs 2 to 4 of this Part B shall apply if the Contract has been specified as a Critical Service Contract under Paragraph 1.1 of this Part B or the Supplier is or becomes a Public Sector Dependent Supplier.
- 2.2 Subject to Paragraphs 2.6, 2.10 and 2.11 of this Part B:
 - 2.2.1 where the Contract is a Critical Service Contract, the Supplier shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the Effective Date; and
 - 2.2.2 except where it has already been provided, where the Supplier is a Public Sector Dependent Supplier, it shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the date of the Appropriate Authority's or Appropriate Authorities' request.
- 2.3 The Supplier shall ensure that the CRP Information provided pursuant to Paragraphs 2.2, 2.8 and 2.9 of this Part B:
 - 2.3.1 is full, comprehensive, accurate and up to date;
 - 2.3.2 is split into two parts:
 - (a) Group Structure Information and Resolution Commentary;
 - (b) UK Public Service / CNI Contract Information and is structured and presented in accordance with the requirements and explanatory notes set out at Annex I of the latest published version of the Resolution Planning Guidance published by the Cabinet Office Government Commercial Function and available at <https://www.gov.uk/government/publications/the-outsourcingplaybook> and contains the level of detail required (adapted as necessary to the Supplier's circumstances);
 - 2.3.3 incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Appropriate Authority or Appropriate Authorities to understand and consider the information for approval;
 - 2.3.4 provides a clear description and explanation of the Supplier Group members that have agreements for goods, services or works provision

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

- in respect of UK Public Sector Business and/or Critical National Infrastructure and the nature of those agreements; and
- 2.3.5 complies with the requirements set out at Appendix 1 (Group Structure Information and Resolution Commentary) and Appendix 2 (UK Public Sector / CNI Contract Information) respectively.
- 2.4 Following receipt by the Appropriate Authority or Appropriate Authorities of the CRP Information pursuant to Paragraphs 2.2, 2.8 and 2.9 of this Part B, the Buyer shall procure that the Appropriate Authority or Appropriate Authorities shall discuss in good faith the contents of the CRP Information with the Supplier and no later than 60 days after the date on which the CRP Information was delivered by the Supplier either provide an Assurance to the Supplier that the Appropriate Authority or Appropriate Authorities approves the CRP Information or that the Appropriate Authority or Appropriate Authorities rejects the CRP Information.
- 2.5 If the Appropriate Authority or Appropriate Authorities rejects the CRP Information:
- 2.5.1 the Buyer shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Supplier in writing of its reasons for its rejection; and
- 2.5.2 the Supplier shall revise the CRP Information, taking reasonable account of the Appropriate Authority's or Appropriate Authorities' comments, and shall re-submit the CRP Information to the Appropriate Authority or Appropriate Authorities for approval within 30 days of the date of the Appropriate Authority's or Appropriate Authorities' rejection. The provisions of paragraph 2.3 to 2.5 of this Part B shall apply again to any resubmitted CRP Information provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure under Clause 34 of the Core Terms at any time.
- 2.6 Where the Supplier or a member of the Supplier Group has already provided CRP Information to a Department or the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that Department and the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid (which has the meaning in paragraph 2.7 below) on the date by which the CRP Information would otherwise be required, the Supplier shall not be required to provide the CRP Information under Paragraph 2.2 if it provides a copy of the Valid Assurance to the Appropriate Authority or Appropriate Authorities on or before the date on which the CRP Information would otherwise have been required.
- 2.7 An Assurance shall be deemed Valid for the purposes of Paragraph 2.6 of this Part B if:
- 2.7.1 the Assurance is within the validity period stated in the Assurance (or, if no validity period is stated, no more than 12 months has elapsed since

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

- it was issued and no more than 18 months has elapsed since the Accounting Reference Date on which the CRP Information was based); and
- 2.7.2 no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if the Contract had then been in force) have occurred since the date of issue of the Assurance.
- 2.8 If the Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 2.8.3 of this Part B its initial CRP Information) to the Appropriate Authority or Appropriate Authorities:
- 2.8.1 within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 2.11 of this Part B) unless the Supplier is relieved of the consequences of the Financial Distress Event under Paragraph 7.1 of Joint Schedule 7 (Financial Distress) (if applicable);
- 2.8.2 within 30 days of a Corporate Change Event unless not required pursuant to Paragraph 2.10;
- 2.8.3 within 30 days of the date that:
- (a) the credit rating(s) of each of the Supplier and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 2.10; or
 - (b) none of the credit rating agencies specified at Paragraph 2.10 hold a public credit rating for the Supplier or any of its Parent Undertakings; and
- 2.8.4 in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Appropriate Authority (whichever is the earlier), unless:
- (a) updated CRP Information has been provided under any of Paragraphs 2.8.1 2.8.2 or 2.8.3 since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 2.8.4; or
 - (b) unless not required pursuant to Paragraph 2.10.
- 2.9 Where the Supplier is a Public Sector Dependent Supplier and the Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 2.8.1 to 2.8.4 of this Part B, the Supplier shall provide at the request of the Appropriate Authority or Appropriate Authorities and within the applicable timescales for each event as set out in Paragraph 2.8 (or such longer timescales as may be notified to the Supplier by the Buyer), the CRP Information to the Appropriate Authority or Appropriate Authorities.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

- 2.10 Where the Supplier or a Parent Undertaking of the Supplier has a credit rating of either:

2.10.1 Aa3 or better from Moody's;

2.10.2 AA- or better from Standard and Poors;

2.10.3 AA- or better from Fitch;

the Supplier will not be required to provide any CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Supplier is relieved of the consequences of the Financial Distress Event under Paragraph 7.1 of Annex 3 to Joint Schedule 7 (Financial Distress), if applicable) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 2.10, in which cases the Supplier shall provide the updated version of the CRP Information in accordance with paragraph 2.8.

- 2.11 Subject to Paragraph 4, where the Supplier demonstrates to the reasonable satisfaction of the Appropriate Authority or Appropriate Authorities that a particular item of CRP Information is highly confidential, the Supplier may, having orally disclosed and discussed that information with the Appropriate Authority or Appropriate Authorities, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Supplier shall promptly provide the relevant information to the Appropriate Authority or Appropriate Authorities to the extent required under Paragraph 2.8.

3. Termination Rights

- 3.1 The Buyer shall be entitled to terminate the Contract if the Supplier is required to provide CRP Information under Paragraph 2 of this Part B and either:

3.1.1 the Supplier fails to provide the CRP Information within 4 months of the Effective Date if this is a Critical Service Contract or otherwise within 4 months of the Appropriate Authority's or Appropriate Authorities' request; or

3.1.2 the Supplier fails to obtain an Assurance from the Appropriate Authority or Appropriate Authorities within 4 months of the date that it was first required to provide the CRP Information under the Contract,

which shall be deemed to be an event to which Clause 10.4.1 of the Core Terms applies and Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply accordingly.

4. Confidentiality and usage of CRP Information

- 4.1 The Buyer agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Supplier and/or Supplier Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

- 4.2 Where the Appropriate Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier's request, the Buyer shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Supplier containing terms no less stringent than those placed on the Buyer under paragraph 4.1 of this Part B and Clause 15 of the Core Terms.
- 4.3 The Supplier shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Appropriate Authority or Appropriate Authorities pursuant to Paragraph 2 of this Part B subject, where necessary, to the Appropriate Authority or Appropriate Authorities entering into an appropriate confidentiality agreement in the form required by the third party.
- 4.4 Where the Supplier is unable to procure consent pursuant to Paragraph 4.3 of this Part B, the Supplier shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by:
- 4.4.1 redacting only those parts of the information which are subject to such obligations of confidentiality;
 - 4.4.2 providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:
 - (a) summarising the information;
 - (b) grouping the information;
 - (c) anonymising the information; and
 - (d) presenting the information in general terms
- 4.5 The Supplier shall provide the Appropriate Authority or Appropriate Authorities with contact details of any third party which has not provided consent to disclose CRP Information where that third party is also a public sector body and where the Supplier is legally permitted to do so.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

Appendix 1: Group structure information and resolution commentary

1. The Supplier shall:
 - 1.1 provide sufficient information to allow the Appropriate Authority to understand the implications on the Supplier Group's UK Public Sector Business and CNI contracts listed pursuant to Appendix 2 if the Supplier or another member of the Supplier Group is subject to an Insolvency Event;
 - 1.2 ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Supplier Group; and
 - 1.3 provide full details of the importance of each member of the Supplier Group to the Supplier Group's UK Public Sector Business and CNI contracts listed pursuant to Appendix 2 and the dependencies between each.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

Appendix 2: UK Public Sector / CNI Contract Information

1. The Supplier shall:
 - 1.1 provide details of all agreements held by members of the Supplier Group where those agreements are for goods, services or works provision and:
 - 1.1.1 are with any UK public sector bodies including: central Government departments and their arms-length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police fire and rescue, education bodies and the devolved administrations;
 - 1.1.2 are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in paragraph 1.1.1 of this Appendix 2 and where the member of the Supplier Group is acting as a key sub-contractor under the agreement with the end recipient; or
 - 1.1.3 involve or could reasonably be considered to involve CNI;
 - 1.2 provide the Appropriate Authority with a copy of the latest version of each underlying contract worth more than £5m per contract year and their related key sub-contracts, which shall be included as embedded documents within the CRP Information or via a directly accessible link.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements

1. Definitions

- 1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Breach of Security"	<p>1 the occurrence of:</p> <p>a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or</p> <p>b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,</p> <p>2 in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;</p>
"Security Management Plan"	<p>3 the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.</p>

2. Complying with security requirements and updates to them

- 2.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

- 2.2 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.
- 2.3 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.
- 2.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.
- 2.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

- 3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.
- 3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:
 - 3.2.1 is in accordance with the Law and this Contract;
 - 3.2.2 as a minimum demonstrates Good Industry Practice;
 - 3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and
 - 3.2.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.
- 3.3 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.
- 3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

4. Security Management Plan**4.1 Introduction**

- 4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

4.2 Content of the Security Management Plan

4.2.1 The Security Management Plan shall:

- a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;
- b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
- c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
- d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
- e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;
- f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and
- g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

4.3 Development of the Security Management Plan

- 4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.
- 4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.
- 4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.
- 4.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

4.4 Amendment of the Security Management Plan

- 4.4.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:
- a) emerging changes in Good Industry Practice;
 - b) any change or proposed change to the Deliverables and/or associated processes;
 - c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;
 - d) any new perceived or changed security threats; and
 - e) any reasonable change in requirements requested by the Buyer.
- 4.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

- a) suggested improvements to the effectiveness of the Security Management Plan;
- b) updates to the risk assessments; and
- c) suggested improvements in measuring the effectiveness of controls.

4.4.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

4.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

5. Security breach

5.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

- 5.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:
- a) minimise the extent of actual or potential harm caused by any Breach of Security;
 - b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;
 - c) prevent an equivalent breach in the future exploiting the same cause failure; and
 - d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

attempted Breach of Security, including a cause analysis where required by the Buyer.

- 5.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

Part B: Long Form Security Requirements

NOT APPLICABLE

1. Definitions

1.1 In this Schedule the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

<p>"Breach of Security"</p>	<p>4 means the occurrence of:</p> <ul style="list-style-type: none"> a) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, <p>5 in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;</p>
<p>"ISMS"</p>	<p>6 the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and</p>
<p>"Security Tests"</p>	<p>7 tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.</p>

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

2. Security Requirements

2.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

2.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

2.3.1 insert security representative of the Buyer

2.3.2 [REDACTED]

2.4 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.5 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

2.6 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.

2.7 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

2.8 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

3. Information Security Management System (ISMS)

3.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.

3.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

3.3 The Buyer acknowledges that;

3.3.1 If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

an extant ISMS covering the Services and their implementation across the Supplier's estate; and

- 3.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.

3.4 The ISMS shall:

- 3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;
- 3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;
- 3.4.3 at all times provide a level of security which:
- a) is in accordance with the Law and this Contract;
 - b) complies with the Baseline Security Requirements;
 - c) as a minimum demonstrates Good Industry Practice;
 - d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;
 - e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4)
(<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>)
 - f) takes account of guidance issued by the Centre for Protection of National Infrastructure
(<https://www.cpni.gov.uk>)
 - g) complies with HMG Information Assurance Maturity Model and Assurance Framework
(<https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm>)
 - h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;
 - i) addresses issues of incompatibility with the Supplier's own organisational security policies; and
 - j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

- 3.4.4 document the security incident management processes and incident response plans;
 - 3.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and
 - 3.4.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).
- 3.5 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.
- 3.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.
- 3.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.
- 3.8 Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

4. Security Management Plan

4.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

- 4.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);
- 4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;
- 4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;
- 4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;
- 4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
- 4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);
- 4.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

example, 'platform as a service' offering from the G-Cloud catalogue);

- 4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;
- 4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;
- 4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and
- 4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5. Amendment of the ISMS and Security Management Plan

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:

- 5.1.1 emerging changes in Good Industry Practice;
- 5.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;
- 5.1.3 any new perceived or changed security threats;

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

- 5.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;
 - 5.1.5 any new perceived or changed security threats; and
 - 5.1.6 any reasonable change in requirement requested by the Buyer.
- 5.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:
- 5.2.1 suggested improvements to the effectiveness of the ISMS;
 - 5.2.2 updates to the risk assessments;
 - 5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and
 - 5.2.4 suggested improvements in measuring the effectiveness of controls.
- 5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.
- 5.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

6. Security Testing

- 6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.
- 6.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

- 6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.
- 6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.
- 6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. Complying with the ISMS

- 7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.
- 7.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.
- 7.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

8. Security Breach

8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

8.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

- a) minimise the extent of actual or potential harm caused by any Breach of Security;
- b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;
- c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;
- d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and
- e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and
- f) as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

of Security, including a root cause analysis where required by the Buyer.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

9. Vulnerabilities and fixing them

9.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

9.2 The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST <http://nvd.nist.gov/cvss.cfm>); and

9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

9.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or

9.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

9.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

9.4.2 is agreed with the Buyer in writing.

9.5 The Supplier shall:

9.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

9.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

9.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;

9.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

9.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

9.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and

9.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

9.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

Part B – Annex 1:**Baseline security requirements****1. Handling Classified information**

- 1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2. End user devices

- 2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre ("NCSC") to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").
- 2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (<https://www.ncsc.gov.uk/guidance/end-user-device-security>). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. Data Processing, Storage, Management and Destruction

- 3.1 The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.
- 3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

3.3 The Supplier shall:

- 3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;
- 3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;
- 3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and
- 3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

- 4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.
- 4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. Security by design

- 5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.
- 5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (<https://www.ncsc.gov.uk/section/products-services/ncsc-certification>) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

- 6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.
- 6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.
- 6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

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

6.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

8. Audit

8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

Part B – Annex 2 - Security Management Plan

To be agreed by the Parties.

Call-Off Schedule 15 (Call-Off Contract Management)

Call-Off Ref:

Crown Copyright 2018

Call-Off Schedule 15 (Call-Off Contract Management)

1. DEFINITIONS

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Operational Board"	the board established in accordance with paragraph 4.1 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. PROJECT MANAGEMENT

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager's shall be:

- 3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;
- 3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;
- 3.1.3 able to cancel any delegation and recommence the position himself; and
- 3.1.4 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager's in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

Call-Off Schedule 15 (Call-Off Contract Management)

Call-Off Ref:

Crown Copyright 2018

- 3.3 Receipt of communication from the Supplier's Contract Manager's by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. ROLE OF THE OPERATIONAL BOARD

- 4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.
- 4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.
- 4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.
- 4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.
- 4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

5. Contract Risk Management

- 5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.
- 5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:
- 5.2.1 the identification and management of risks;
 - 5.2.2 the identification and management of issues; and
 - 5.2.3 monitoring and controlling project plans.
- 5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.
- 5.4 The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer's and the Supplier have identified.

Call-Off Schedule 15 (Call-Off Contract Management)

Call-Off Ref:

Crown Copyright 2018

Annex: Contract Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

Weekly Sprint meetings

- To discuss developments and improvements of the service
- Held between Immersive Labs, SIO, Live services and communications

Bi-monthly Supplier Reviews (every 2 months)

- To discuss service performance and reporting
- Held between Immersive Labs, SIO, Live services, communications, and regional leads

Annual Business Review

- To discuss strategic and a roundup of key operational activities
- Immersive Labs, SIO, Live services, communications, regional leads and management

Call-Off Schedule 15 (Call-Off Contract Management)

Call-Off Ref:

Crown Copyright 2018

Call-Off Schedule 16 (Benchmarking)

Call-Off Ref:

Crown Copyright 2018

Call-Off Schedule 16 (Benchmarking)**1. DEFINITIONS**

1.1 In this Schedule, the following expressions shall have the following meanings:

"Benchmark Review"	a review of the Deliverables carried out in accordance with this Schedule to determine whether those Deliverables represent Good Value;
"Benchmarked Deliverables"	any Deliverables included within the scope of a Benchmark Review pursuant to this Schedule;
"Comparable Rates"	the Charges for Comparable Deliverables;
"Comparable Deliverables"	deliverables that are identical or materially similar to the Benchmarking Deliverables (including in terms of scope, specification, volume and quality of performance) provided that if no identical or materially similar Deliverables exist in the market, the Supplier shall propose an approach for developing a comparable Deliverables benchmark;
"Comparison Group"	a sample group of organisations providing Comparable Deliverables which consists of organisations which are either of similar size to the Supplier or which are similarly structured in terms of their business and their service offering so as to be fair comparators with the Supplier or which, are best practice organisations;
"Equivalent Data"	data derived from an analysis of the Comparable Rates and/or the Comparable Deliverables (as applicable) provided by the Comparison Group;
"Good Value"	that the Benchmarking Rates are within the Upper Quartile; and
"Upper Quartile"	in respect of Benchmarking Rates, that based on an analysis of Equivalent Data, the Benchmarking Rates, as compared to the range of prices for Comparable Deliverables, are within the top 25% in terms of best value for money for the recipients of Comparable Deliverables.

Call-Off Schedule 16 (Benchmarking)

Call-Off Ref:

Crown Copyright 2018

2. When you should use this Schedule

- 2.1 The Supplier acknowledges that the Buyer wishes to ensure that the Deliverables, represent value for money to the taxpayer throughout the Contract Period.
- 2.2 This Schedule sets to ensure the Contracts represent value for money throughout and that the Buyer may terminate the Contract by issuing a Termination Notice to the Supplier if the Supplier refuses or fails to comply with its obligations as set out in Paragraphs 3 of this Schedule.
- 2.3 Amounts payable under this Schedule shall not fall with the definition of a Cost.

3. Benchmarking**3.1 How benchmarking works**

- 3.1.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.
- 3.1.2 The Buyer may, by written notice to the Supplier, require a Benchmark Review of any or all of the Deliverables.
- 3.1.3 The Buyer shall not be entitled to request a Benchmark Review during the first six (6) Month period from the Contract Commencement Date or at intervals of less than twelve (12) Months after any previous Benchmark Review.
- 3.1.4 The purpose of a Benchmark Review will be to establish whether the Benchmarked Deliverables are, individually and/or as a whole, Good Value.
- 3.1.5 The Deliverables that are to be the Benchmarked Deliverables will be identified by the Buyer in writing.
- 3.1.6 Upon its request for a Benchmark Review the Buyer shall nominate a benchmarker. The Supplier must approve the nomination within ten (10) Working Days unless the Supplier provides a reasonable explanation for rejecting the appointment. If the appointment is rejected then the Buyer may propose an alternative benchmarker. If the Parties cannot agree the appointment within twenty (20) days of the initial request for Benchmark review then a benchmarker shall be selected by the Chartered Institute of Financial Accountants.
- 3.1.7 The cost of a benchmarker shall be borne by the Buyer (provided that each Party shall bear its own internal costs of the Benchmark Review) except where the Benchmark Review demonstrates that the Benchmarked Service and/or the Benchmarked Deliverables are not Good Value, in which case

Call-Off Schedule 16 (Benchmarking)

Call-Off Ref:

Crown Copyright 2018

the Parties shall share the cost of the benchmarker in such proportions as the Parties agree (acting reasonably). Invoices by the benchmarker shall be raised against the Supplier and the relevant portion shall be reimbursed by the Buyer.

3.2 Benchmarking Process

- 3.2.1 The benchmarker shall produce and send to the Buyer, for Approval, a draft plan for the Benchmark Review which must include:
- (a) a proposed cost and timetable for the Benchmark Review;
 - (b) a description of the benchmarking methodology to be used which must demonstrate that the methodology to be used is capable of fulfilling the benchmarking purpose; and
 - (c) a description of how the benchmarker will scope and identify the Comparison Group.
- 3.2.2 The benchmarker, acting reasonably, shall be entitled to use any model to determine the achievement of value for money and to carry out the benchmarking.
- 3.2.3 The Buyer must give notice in writing to the Supplier within ten (10) Working Days after receiving the draft plan, advising the benchmarker and the Supplier whether it Approves the draft plan, or, if it does not approve the draft plan, suggesting amendments to that plan (which must be reasonable). If amendments are suggested then the benchmarker must produce an amended draft plan and this Paragraph 3.2.3 shall apply to any amended draft plan.
- 3.2.4 Once both Parties have approved the draft plan then they will notify the benchmarker. No Party may unreasonably withhold or delay its Approval of the draft plan.
- 3.2.5 Once it has received the Approval of the draft plan, the benchmarker shall:
- (a) finalise the Comparison Group and collect data relating to Comparable Rates. The selection of the Comparable Rates (both in terms of number and identity) shall be a matter for the Supplier's professional judgment using:
 - (i) market intelligence;
 - (ii) the benchmarker's own data and experience;
 - (iii) relevant published information; and
 - (iv) pursuant to Paragraph 3.2.6 below, information from other suppliers or purchasers on Comparable Rates;
 - (b) by applying the adjustment factors listed in Paragraph 3.2.7 and from an analysis of the Comparable Rates, derive the Equivalent Data;

Call-Off Schedule 16 (Benchmarking)

Call-Off Ref:

Crown Copyright 2018

- (c) using the Equivalent Data, calculate the Upper Quartile;
 - (d) determine whether or not each Benchmarked Rate is, and/or the Benchmarked Rates as a whole are, Good Value.
- 3.2.6 The Supplier shall use all reasonable endeavours and act in good faith to supply information required by the benchmarker in order to undertake the benchmarking. The Supplier agrees to use its reasonable endeavours to obtain information from other suppliers or purchasers on Comparable Rates.
- 3.2.7 In carrying out the benchmarking analysis the benchmarker may have regard to the following matters when performing a comparative assessment of the Benchmarked Rates and the Comparable Rates in order to derive Equivalent Data:
- (a) the contractual terms and business environment under which the Comparable Rates are being provided (including the scale and geographical spread of the customers);
 - (b) exchange rates;
 - (c) any other factors reasonably identified by the Supplier, which, if not taken into consideration, could unfairly cause the Supplier's pricing to appear non-competitive.

3.3 Benchmarking Report

- 3.3.1 For the purposes of this Schedule "**Benchmarking Report**" shall mean the report produced by the benchmarker following the Benchmark Review and as further described in this Schedule;
- 3.3.2 The benchmarker shall prepare a Benchmarking Report and deliver it to the Buyer, at the time specified in the plan Approved pursuant to Paragraph 3.2.3, setting out its findings. Those findings shall be required to:
- (a) include a finding as to whether or not a Benchmarked Service and/or whether the Benchmarked Deliverables as a whole are, Good Value;
 - (b) if any of the Benchmarked Deliverables are, individually or as a whole, not Good Value, specify the changes that would be required to make that Benchmarked Service or the Benchmarked Deliverables as a whole Good Value; and
 - (c) include sufficient detail and transparency so that the Party requesting the Benchmarking can interpret and understand how the Supplier has calculated whether or not the Benchmarked Deliverables are, individually or as a whole, Good Value.
- 3.3.3 The Parties agree that any changes required to this Contract identified in the Benchmarking Report shall be implemented at

Call-Off Schedule 16 (Benchmarking)

Call-Off Ref:

Crown Copyright 2018

the direction of the Buyer in accordance with Clause 24
(Changing the contract).

Call-Off Schedule 16 (Benchmarking)

Call-Off Ref:

Crown Copyright 2018

Call-Off Schedule 20 (Call-Off Specification)
Call-Off Ref:
Crown Copyright 2018

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract

prj_C244015: Cyber Workforce Training Platform

Requirement

Please could you provide a quote and lead time(s) / delivery timescale(s) for the following Cyber Workforce Training Platform (www.immersivelabs.com) – Immersive Labs Enterprise-wide licence product/ service requirement, using the reference number provided.

All bids must be attached to the ITT registered on the NHS England's Atamis portal.

Overview

NHS England's Transformation Directorate (formerly NHS Digital) is a ground-breaking data, information and technology resource for the health and social care system and plays a fundamental role in driving better care, better services, and better outcomes for patients.

We collect, analyse, and publish national data and statistical information. We deliver national IT systems and services to support the health and social care system.

This document is for the provision of summarised products in the table below:

Summary of products

Product / Service	Number	Description
Cyber Professional Licences	Enterprise-wide license	2000+ world leading Cyber Security on demand labs with the catalogue growing weekly
		Includes a Customer Success Manager who will support with everyday tasks such as licencing and basic reporting
App Sec Cloud Sec	Enterprise-wide license	The aim is to leverage data insights to strengthen the software development life cycle and reduce vulnerabilities in applications

Call-Off Schedule 20 (Call-Off Specification)

Call-Off Ref:

Crown Copyright 2018

Crisis Simulation Tool	Enterprise-wide license	Access to a library of cyber incident response scenarios and ability to custom build own scenarios relevant to work area. Catalogue of scenarios is continuously added to
Screening	Enterprise-wide license	Allows managers to effectively tailor job advertisements to specific technical roles and then test candidates' technical ability before interview. For internal or external candidates
Team Sim	10 Credits	Prove the effectiveness of Red and Blue Teams as they progress through complex technical scenarios.
Cyber Workforce Advisor	1 Full Time Dedicated	Full time resource attached to account to drive engagement and ensure successful outcomes. Employed by Immersive Labs, but very much embedded into the NHS

Background

The Immersive Labs platform is an enterprise offering aligned to the challenges faced by complex organisations with a people-centric approach. This happens by the platform offering continually evolving utilising the knowledge of the Immersive Labs team but equally important customer feedback. It is this partnership that enables Immersive labs to evolve in an agile manner to keep abreast of the ever-changing cyber landscape.

The real-time reporting feature on the Immersive Labs platform, combined with the ability to nest NHS teams, enables organisations to evidence value and establish a standard of cyber resilience across multiple products. Achieving this through being accessible for all skill sets, empowering the neurodiverse, being inclusive and breaking down geographical boundaries

Service Users

This service will be consumed by any member of the NHS community through the purchase of an enterprise-wide license. It helps NHS England achieve one of its ambitions on building a cyber resilience workforce and culture. Currently there are 2380 users registered and 66% of them have used immersive labs between April

Call-Off Schedule 20 (Call-Off Specification)
Call-Off Ref:
Crown Copyright 2018

2023 to November 2023. Aspiration is to grow both register users but users actually using the system over the coming years.

Products and Benefits

By undertaking this procurement, we hope to deliver the following products and outcomes to the NHS system.

Hands on Labs – Cyber Pro

Immersive Labs provides extensive coverage of topics for cybersecurity professionals, developers and infrastructure engineers, as well as the wider workforce, with over 2,300 labs across multiple categories. Labs spin up in the browser on demand and can be accessed wherever the employee is and at any time.

Immersive Labs uses the latest gamified techniques and live environments to learn topics from security fundamentals to malware reverse engineering and advanced threat hunting. This provides the following benefits:

- Improve individual and team cybersecurity capabilities across a comprehensive range of subjects.
- Benchmark and prove current levels of cyber capabilities across the NHS.
- Demonstrate team ability aligned to security frameworks (e.g., MITRE ATT&CK)
- Improve speed of response to emerging threats
- Increase efficacy in recruitment, retention, and promotion.
- Reduce vulnerabilities early and across the software development lifecycle.
- Securely configure cloud workloads
- Enhancement of current NHSE Cyber operations portfolio by sharing of lessons learned to create new labs and use existing labs to support other products e.g. labs focused on phishing following a simulation.
- Improve training outcomes across the NHS delivering at scale to a diverse workforce and improve the overall cyber resilience.

Immersive Labs has a constantly growing catalogue for beginner, intermediate, and the most advanced audiences, and is a one of the market leaders in this space, covering a broad spectrum of skill sets as required by the NHS. As the catalogue of labs grows, we are seeing an ever-increasing number of individuals requesting access from a diverse workforce. We have registered 2380 users and 66% of them have used immersive labs between April 2023 to November 2023.

NHS currently have 12 bespoke career pathways curated and aligned to the Cyber 3 strategy with new ones in the pipeline, those available include.

- Keep IT Confidential aligned content.

Call-Off Schedule 20 (Call-Off Specification)

Call-Off Ref:

Crown Copyright 2018

- Cyber Associates Network Custom Roles
 - Non-technical
 - Entry technical
 - Foundational technical
 - Intermediate technical
 - Advanced technical
- Security Champions Network (4 parts)
- NHS Multi Factor Authentication collection
- Custom content collection for York and Scarborough Teaching Hospitals NHS Foundation Trust

We ensure the labs are always up to date, with the latest Cyber Threat Intelligence labs being released into the platform often within 24 hours of the threat being identified, enabling staff to begin to understand and mitigate any risks to their systems. Such speed to market with these labs is unique to Immersive Labs.

There is detailed evidence-based performance data for both individuals and teams which will help the NHS understand, baseline, benchmark, and prove their cyber capabilities to their boards and Government.

Application and Cloud Security

The demands of the NHS today mean applications are being built quicker than ever. Often such business demands mean an increase in the likelihood of software vulnerabilities.

Immersive Labs measures and enhances development teams' security capabilities across the entire software development lifecycle. In order to learn, Immersive Labs provides teams with a wide range of common security errors in code and configurations to identify and fix. By offering hands-on AppSec experiences, your teams' knowledge, skills, and judgment on secure coding, secure operations, and secure testing will improve. The benefits are:

- Developers are able to quickly identify and fix vulnerabilities, increasing productivity.
- NHS are able to hire and upskill junior developers and DevSecOps professionals to reduce hiring costs.
- NHS can save money by identifying vulnerabilities earlier in the SDLC.
- Addresses compliance mandates related to secure coding.

Crisis Sim

Traditional methods of testing crisis preparedness are linear, unengaging, and not data driven.

Call-Off Schedule 20 (Call-Off Specification)
Call-Off Ref:
Crown Copyright 2018

Based on the latest cyber threats, Immersive Labs's cloud-based Crisis Simulations provide Boards, executives, and crisis management teams with realistic exercises to measure and improve executive confidence, knowledge and decision-making in managing cyber risk and operational resilience. Out-of-the-box scenarios deliver severe but plausible exercises for numerous types of crises and industries.

In-depth simulations reflect how real-life crises unfold, while removing the logistical burdens of in-person exercises - ideal for nationally dispersed teams such as the NHS.

The Crisis Sim is fully customisable so NHS can make and deliver their own exercises relevant to their needs to unlimited audiences. With bespoke content such as crisis sims aligned to DSPT enabling NHS to evidence multiple controls through the learning platform. 2024 sees IL enabling NHS to evidence preparedness in line with the Cyber Assessment Framework.

NHS has benefited from running catalogue exercises that can be assigned and run as individuals or played in a presentation mode face to face or via online webinar NHS has also run multiple curated events which have proved immensely useful for events such as cyber awareness month. The benefits are:

- Develop muscle memory to handle cyber incidents.
- Providing a safe environment to test an organisations cyber incident response process.
- The ability to validate roles and responsibilities, including deputies, and communication channels.

Team Sim

Immersive Labs provides the ability to exercise your teams' capabilities in complex environments that are representative of what they experience in their day-to-day operations. These provide security teams with preconfigured, task-based, technical simulations that enable teams to collaborate through real-world scenarios.

The benefits are:

- Regular practice in realistic scenarios helps your teams perform optimally when real incidents occur
- Practice more frequently using always-available scenarios that you can use in minutes
- Prove team performance and build confidence that your people are prepared to respond to the latest threats

Call-Off Schedule 20 (Call-Off Specification)

Call-Off Ref:

Crown Copyright 2018

- Identify gaps in current knowledge and show team improvement over time, confirming ROI on upskilling

Screening

The screening tool enables the NHS to test potential applicants against the specific skills required for an open cybersecurity position.

Immersive Labs' hands-on challenges enable remote testing of relevant technical abilities before advancing a candidate to the interview stage. And because our labs simulate real-world scenarios, the NHS can test how well a candidate might actually perform in the job – and under pressure.

Quality

Product Requirement

Through the close working relationship with the customer workforce advisor, we will aim to maximise the value of the product through the curation of custom labs and support in developing crisis sim labs.

Through regular review meetings we will gain an understanding of immersive labs product roadmap, and take advantage of products that will add value as part of our existing enterprise license.

Maintenance and Support

The day-to-day operations of the product and the creation and setup of users will be done by the NHS England 2nd line team. The customer workforce advisor will provide support around improving the value of the product for NHS England through aligning to our strategy and working with us to incorporate feature enhancements to the platform.

Delivery

Upon setup of the contracts, Immersive labs will need to provide confirmation that the unique coupon code is still valid for the NHS account already setup.

This code will allow the NHS England 2nd line team to register and add new users to the NHS account, allowing them access to the products purchased.

Call-Off Schedule 20 (Call-Off Specification)
Call-Off Ref:
Crown Copyright 2018

Implementation

The NHS account has already been setup on the Immersvie labs platform, the only check that is needed will be to ensure the unique coupon code is still correct that will allow us to setup new users on the platform and access the products

Asseting

Software Licenses: Each separate software license will require a record for asset management.

For each license purchased, the following should be sent to NHS England:

- Proof of license – i.e. license certificate
- Manufacturer
- Entitlement details:
 - Product Entitlement(s)
 - Edition Entitlement(s)
 - Version Entitlement(s)
- License Type – e.g. Per User, Per Device, Concurrent, Node-locked etc.
- Start and End Dates for Entitlements, if applicable
- Part Code / Product SKU (if available)
- Serial number / License Identification Numbers
- Associated agreement numbers
- Licence key
- Price (excluding maintenance)
- Delivery Date
- Maintenance costs
- Maintenance start and end dates

Where the license price is not free or be separated from the first period of maintenance, please indicate if the maintenance is free, or advise of the equivalent cost of maintenance for the same period, if purchased separately.

Environmental

The supply of the requested products must be compliant with EC Green Public Procurement (GPP) regulations. Further details are available [here](#). In your response, also include details of any other regulations / standard that the requested products are compliant to.

Any additional environmental added value which can be demonstrated will be considered in evaluating proposals put forward.

Call-Off Schedule 20 (Call-Off Specification)
Call-Off Ref:
Crown Copyright 2018

Cyber Essentials Plus

Cyber Essentials plus certification is required.

Costs

NHS England will be evaluating the proposed solution on affordability and value for money. As such, costs for the following should be included in the price along with the product/ service deliverable as a minimum:

- Initial outlay
- Delivery services – including implementation.
- On-going support and maintenance

Term

- Commencing 1st July 2024 for 12 months with an option to extend for further 12 months

Call-Off Schedule 20 (Call-Off Specification)
Call-Off Ref:
Crown Copyright 2018



Crown
Commercial
Service

Core Terms - RM6098

1. Definitions used in the contract

Interpret this Contract using Joint Schedule 1 (Definitions).

2. How the contract works

- 2.1 The Supplier is eligible for the award of Call-Off Contracts during the Framework Contract Period.
- 2.2 CCS does not guarantee the Supplier any exclusivity, quantity or value of work under the Framework Contract.
- 2.3 CCS has paid one penny to the Supplier legally to form the Framework Contract. The Supplier acknowledges this payment.
- 2.4 If the Buyer decides to buy Deliverables under the Framework Contract it must use Framework Schedule 7 (Call-Off Award Procedure) and must state its requirements using Framework Schedule 6 (Order Form Template and Call-Off Schedules). If allowed by the Regulations, the Buyer can:
 - (a) make changes to Framework Schedule 6 (Order Form Template and Call-Off Schedules);
 - (b) create new Call-Off Schedules;
 - (c) exclude optional template Call-Off Schedules; and/or
 - (d) use Special Terms in the Order Form to add or change terms.
- 2.5 Each Call-Off Contract:
 - (a) is a separate Contract from the Framework Contract;
 - (b) is between a Supplier and a Buyer;
 - (c) includes Core Terms, Schedules and any other changes or items in the completed Order Form; and
 - (d) survives the termination of the Framework Contract.
- 2.6 Where the Supplier is approached by any Other Contracting Authority requesting Deliverables or substantially similar goods or services, the Supplier must tell them about this Framework Contract before accepting their order.
- 2.7 The Supplier acknowledges it has all the information required to perform its obligations under each Contract before entering into a Contract. When information is provided by a Relevant Authority no warranty of its accuracy is given to the Supplier.
- 2.8 The Supplier will not be excused from any obligation, or be entitled to additional Costs or Charges because it failed to either:
 - (a) verify the accuracy of the Due Diligence Information; or
 - (b) properly perform its own adequate checks.

- 2.9 CCS and the Buyer will not be liable for errors, omissions or misrepresentation of any information.
- 2.10 The Supplier warrants and represents that all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

3. What needs to be delivered

3.1 All deliverables

- 3.1.1 The Supplier must provide Deliverables:
- (a) that comply with the Specification, the Framework Tender Response and, in relation to a Call-Off Contract, the Call-Off Tender (if there is one);
 - (b) to a professional standard;
 - (c) using reasonable skill and care;
 - (d) using Good Industry Practice;
 - (e) using its own policies, processes and internal quality control measures as long as they do not conflict with the Contract;
 - (f) on the dates agreed; and
 - (g) that comply with Law.
- 3.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days from Delivery against all obvious defects.

3.2 Goods clauses

- 3.2.1 All Goods delivered must be new, or as new if recycled or refurbished, and of known origin and authenticity.
- 3.2.2 All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.
- 3.2.3 The Supplier transfers ownership of the Goods on Delivery or payment for those Goods, whichever is earlier.
- 3.2.4 Risk in the Goods transfers to the Buyer on Delivery of the Goods, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.
- 3.2.5 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.
- 3.2.6 The Supplier must deliver the Goods on the date and to the specified location during the Buyer's working hours.

- 3.2.7 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.
- 3.2.8 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.
- 3.2.9 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.
- 3.2.10 The Supplier must indemnify the Buyer against the costs of any Recall of the Goods and give notice of actual or anticipated action about the Recall of the Goods.
- 3.2.11 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable steps to minimise these costs.
- 3.2.12 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they do not conform with Clause 3. If the Supplier does not do this it will pay the Buyer's costs including repair or re-supply by a third party.

3.3 Services clauses

- 3.3.1 Late Delivery of the Services will be a Default of a Call-Off Contract.
- 3.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the Delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions.
- 3.3.3 The Supplier must at its own risk and expense provide all Supplier Equipment required to Deliver the Services.
- 3.3.4 The Supplier must allocate sufficient resources and appropriate expertise to each Contract.
- 3.3.5 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.
- 3.3.6 The Supplier must ensure all Services, and anything used to Deliver the Services, are of good quality and free from defects.
- 3.3.7 The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

4. Pricing and payments

- 4.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the Charges in the

Order Form.

- 4.2 CCS must invoice the Supplier for the Management Charge and the Supplier must pay it using the process in Framework Schedule 5 (Management Charges and Information).
- 4.3 All Charges and the Management Charge:
- (a) exclude VAT, which is payable on provision of a valid VAT invoice; and
 - (b) include all costs connected with the Supply of Deliverables.
- 4.4 The Buyer must pay the Supplier the Charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds using the payment method and details stated in the Order Form.
- 4.5 A Supplier invoice is only valid if it:
- (a) includes all appropriate references including the Contract reference number and other details reasonably requested by the Buyer;
 - (b) includes a detailed breakdown of Delivered Deliverables and Milestone(s) (if any); and
 - (c) does not include any Management Charge (the Supplier must not charge the Buyer in any way for the Management Charge).
- 4.6 The Buyer must accept and process for payment an undisputed Electronic Invoice received from the Supplier.
- 4.7 The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.
- 4.8 The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this does not happen, CCS or the Buyer can publish the details of the late payment or non-payment.
- 4.9 If CCS or the Buyer can get more favourable commercial terms for the supply at cost of any materials, goods or services used by the Supplier to provide the Deliverables, then CCS or the Buyer may require the Supplier to replace its existing commercial terms with the more favourable terms offered for the relevant items.
- 4.10 If CCS or the Buyer uses Clause 4.9 then the Framework Prices (and where applicable, the Charges) must be reduced by an agreed amount by using the Variation Procedure.
- 4.11 The Supplier has no right of set-off, counterclaim, discount or abatement unless they are ordered to do so by a court.

5. The buyer's obligations to the supplier

- 5.1 If Supplier Non-Performance arises from an Authority Cause:

- (a) neither CCS or the Buyer can terminate a Contract under Clause 10.4.1;
- (b) the Supplier is entitled to reasonable and proven additional expenses and to relief from liability and Deduction under this Contract;
- (c) the Supplier is entitled to additional time needed to make the Delivery; and
- (d) the Supplier cannot suspend the ongoing supply of Deliverables.

5.2 Clause 5.1 only applies if the Supplier:

- (a) gives notice to the Party responsible for the Authority Cause within 10 Working Days of becoming aware;
- (b) demonstrates that the Supplier Non-Performance would not have occurred but for the Authority Cause; and
- (c) mitigated the impact of the Authority Cause.

6. Record keeping and reporting

6.1 The Supplier must attend Progress Meetings with the Buyer and provide Progress Reports when specified in the Order Form.

6.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract:

- (a) during the Contract Period;
- (b) for 7 years after the End Date; and
- (c) in accordance with UK GDPR,

including but not limited to the records and accounts stated in the definition of Audit in Joint Schedule 1.

6.3 The Relevant Authority or an Auditor can Audit the Supplier.

6.4 During an Audit, the Supplier must:

- (a) allow the Relevant Authority or any Auditor access to their premises to verify all contract accounts and records of everything to do with the Contract and provide copies for an Audit; and
- (b) provide information to the Relevant Authority or to the Auditor and reasonable co-operation at their request.

6.5 Where the Audit of the Supplier is carried out by an Auditor, the Auditor shall be entitled to share any information obtained during the Audit with the Relevant Authority.

6.6 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

- (a) tell the Relevant Authority and give reasons;
 - (b) propose corrective action; and
 - (c) provide a deadline for completing the corrective action.
- 6.7 The Supplier must provide CCS with a Self Audit Certificate supported by an audit report at the end of each Contract Year. The report must contain:
- (a) the methodology of the review;
 - (b) the sampling techniques applied;
 - (c) details of any issues; and
 - (d) any remedial action taken.
- 6.8 The Self Audit Certificate must be completed and signed by an auditor or senior member of the Supplier's management team that is qualified in either a relevant audit or financial discipline.

7. Supplier staff

- 7.1 The Supplier Staff involved in the performance of each Contract must:
- (a) be appropriately trained and qualified;
 - (b) be vetted using Good Industry Practice and the Security Policy; and
 - (c) comply with all conduct requirements when on the Buyer's Premises.
- 7.2 Where a Buyer decides one of the Supplier's Staff is not suitable to work on a contract, the Supplier must replace them with a suitably qualified alternative.
- 7.3 If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach Clause 27.
- 7.4 The Supplier must provide a list of Supplier Staff needing to access the Buyer's Premises and say why access is required.
- 7.5 The Supplier indemnifies CCS and the Buyer against all claims brought by any person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8. Rights and protection

- 8.1 The Supplier warrants and represents that:
- (a) it has full capacity and authority to enter into and to perform each Contract;
 - (b) each Contract is executed by its authorised representative;
 - (c) it is a legally valid and existing organisation incorporated in the place it was formed;
 - (d) there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates

- that might affect its ability to perform each Contract;
 - (e) it maintains all necessary rights, authorisations, licences and consents to perform its obligations under each Contract;
 - (f) it does not have any contractual obligations which are likely to have a material adverse effect on its ability to perform each Contract;
 - (g) it is not impacted by an Insolvency Event; and
 - (h) it will comply with each Call-Off Contract.
- 8.2 The warranties and representations in Clauses 2.10 and 8.1 are repeated each time the Supplier provides Deliverables under the Contract.
- 8.3 The Supplier indemnifies both CCS and every Buyer against each of the following:
- (a) wilful misconduct of the Supplier, Subcontractor and Supplier Staff that impacts the Contract; and
 - (b) non-payment by the Supplier of any Tax or National Insurance.
- 8.4 All claims indemnified under this Contract must use Clause 26.
- 8.5 The description of any provision of this Contract as a warranty does not prevent CCS or a Buyer from exercising any termination right that it may have for breach of that clause by the Supplier.
- 8.6 If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify CCS and every Buyer.
- 8.7 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier.

9. Intellectual Property Rights (IPRs)

- 9.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier's Existing IPR to enable it to both:
- (a) receive and use the Deliverables; and
 - (b) make use of the deliverables provided by a Replacement Supplier.
- 9.2 Any New IPR created under a Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs and New IPRs for the purpose of fulfilling its obligations during the Contract Period.
- 9.3 Where a Party acquires ownership of IPRs incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

- 9.4 Neither Party has the right to use the other Party's IPRs, including any use of the other Party's names, logos or trademarks, except as provided in Clause 9 or otherwise agreed in writing.
- 9.5 If there is an IPR Claim, the Supplier indemnifies CCS and each Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.
- 9.6 If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer's sole option, either:
- (a) obtain for CCS and the Buyer the rights in Clause 9.1 and 9.2 without infringing any third party IPR; or
 - (b) replace or modify the relevant item with substitutes that do not infringe IPR without adversely affecting the functionality or performance of the Deliverables.
- 9.7 In spite of any other provisions of a Contract and for the avoidance of doubt, award of a Contract by the Buyer and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949. The Supplier acknowledges that any authorisation by the Buyer under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific IPR involved.

10. Ending the contract or any subcontract

10.1 Contract Period

- 10.1.1 The Contract takes effect on the Start Date and ends on the End Date or earlier if required by Law.
- 10.1.2 The Relevant Authority can extend the Contract for the Extension Period by giving the Supplier no less than 3 Months' written notice before the Contract expires.

10.2 Ending the contract without a reason

- 10.2.1 CCS has the right to terminate the Framework Contract at any time without reason by giving the Supplier at least 30 days' notice.
- 10.2.2 Each Buyer has the right to terminate their Call-Off Contract at any time without reason by giving the Supplier not less than 90 days' written notice.

10.3 Rectification plan process

- 10.3.1 If there is a Default, the Relevant Authority may, without limiting its other rights, request that the Supplier provide a Rectification Plan, within 10 working days .
- 10.3.2 When the Relevant Authority receives a requested Rectification Plan it can either:
- (a) reject the Rectification Plan or revised Rectification Plan, giving reasons; or
 - (b) accept the Rectification Plan or revised Rectification Plan (without limiting its rights) and the Supplier must immediately start work on the actions in the Rectification Plan at its own cost,

unless agreed otherwise by the Parties.

10.3.3 Where the Rectification Plan or revised Rectification Plan is rejected, the Relevant Authority:

- (a) must give reasonable grounds for its decision; and
- (b) may request that the Supplier provides a revised Rectification Plan within 5 Working Days.

10.3.4 If the Relevant Authority rejects any Rectification Plan, including any revised Rectification Plan, the Relevant Authority does not have to request a revised Rectification Plan before exercising its right to terminate its Contract under Clause 10.4.3(a).

10.4 When CCS or the buyer can end a contract

10.4.1 If any of the following events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

- (a) there is a Supplier Insolvency Event;
- (b) there is a Default that is not corrected in line with an accepted Rectification Plan;
- (c) the Supplier does not provide a Rectification Plan within 10 days of the request;
- (d) there is any material Default of the Contract;
- (e) there is any material Default of any Joint Controller Agreement relating to any Contract;
- (f) there is a Default of Clauses 2.10, 9, 14, 15, 27, 32 or Framework Schedule 9 (Cyber Essentials) (where applicable) relating to any Contract;
- (g) there is a consistent repeated failure to meet the Performance Indicators in Framework Schedule 4 (Framework Management);
- (h) there is a Change of Control of the Supplier which is not pre-approved by the Relevant Authority in writing;
- (i) if the Relevant Authority discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded; or
- (j) the Supplier or its Affiliates embarrass or bring CCS or the Buyer into disrepute or diminish the public trust in them.

10.4.2 CCS may terminate the Framework Contract if a Buyer terminates a Call-Off Contract for any of the reasons listed in Clause 10.4.1.

10.4.3 If any of the following non-fault based events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

- (a) the Relevant Authority rejects a Rectification Plan;
- (b) there is a Variation which cannot be agreed using Clause 24 (Changing the contract) or resolved using Clause 34 (Resolving disputes);
- (c) if there is a declaration of ineffectiveness in respect of any Variation; or
- (d) the events in 73 (1) (a) of the Regulations happen.

10.5 When the supplier can end the contract

- 10.5.1 The Supplier can issue a Reminder Notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate a Call-Off Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the annual Contract Value within 30 days of the date of the Reminder Notice.

10.6 What happens if the contract ends

- 10.6.1 Where a Party terminates a Contract under any of Clauses 10.2.1, 10.2.2, 10.4.1, 10.4.2, 10.4.3, 10.5 or 20.2 or a Contract expires all of the following apply:

- (a) The Buyer's payment obligations under the terminated Contract stop immediately.
- (b) Accumulated rights of the Parties are not affected.
- (c) The Supplier must promptly repay to the Buyer any and all Charges the Buyer has paid in advance in respect of Deliverables not provided by the Supplier as at the End Date.
- (d) The Supplier must promptly delete or return the Government Data except where required to retain copies by Law.
- (e) The Supplier must promptly return any of CCS or the Buyer's property provided under the terminated Contract.
- (f) The Supplier must, at no cost to CCS or the Buyer, co-operate fully in the handover and re-procurement (including to a Replacement Supplier).

- 10.6.2 In addition to the consequences of termination listed in Clause 10.6.1, where the Relevant Authority terminates a Contract under Clause 10.4.1 the Supplier is also responsible for the Relevant Authority's reasonable costs of procuring Replacement Deliverables for the rest of the Contract Period.

- 10.6.3 In addition to the consequences of termination listed in Clause 10.6.1, if either the Relevant Authority terminates a Contract under Clause 10.2.1 or 10.2.2 or a Supplier terminates a Call-Off Contract under Clause 10.5:

- (a) the Buyer must promptly pay all outstanding Charges incurred to the Supplier; and
- (b) the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated.

- 10.6.4 In addition to the consequences of termination listed in Clause 10.6.1, where a Party terminates under Clause 20.2 each Party must cover its own Losses.

- 10.6.5 The following Clauses survive the termination or expiry of each Contract: 3.2.10, 4.2, 6, 7.5, 9, 11, 12.2, 14, 15, 16, 17, 18, 31.3, 34, 35 and any Clauses and Schedules which are expressly or by implication intended to continue.

10.7 Partially ending and suspending the contract

- 10.7.1 Where CCS has the right to terminate the Framework Contract it can suspend the Supplier's ability to accept Orders (for any period) and the Supplier cannot enter into any new Call-Off

Contracts during this period. If this happens, the Supplier must still meet its obligations under any existing Call-Off Contracts that have already been signed.

- 10.7.2 Where CCS has the right to terminate a Framework Contract it is entitled to terminate all or part of it.
- 10.7.3 Where the Buyer has the right to terminate a Call-Off Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends a Contract it can provide the Deliverables itself or buy them from a third party.
- 10.7.4 The Relevant Authority can only partially terminate or suspend a Contract if the remaining parts of that Contract can still be used to effectively deliver the intended purpose.
- 10.7.5 The Parties must agree any necessary Variation required by Clause 10.7 using the Variation Procedure, but the Supplier may not either:
- (a) reject the Variation; or
 - (b) increase the Charges, except where the right to partial termination is under Clause 10.2.
- 10.7.6 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under Clause 10.7.

10.8 When subcontracts can be ended

- 10.8.1 At the Buyer's request, the Supplier must terminate any Subcontracts in any of the following events:
- (a) there is a Change of Control of a Subcontractor which is not pre-approved by the Relevant Authority in writing;
 - (b) the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 10.4; or
 - (c) a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Relevant Authority.

11. How much you can be held responsible for

- 11.1 Each Party's total aggregate liability in each Contract Year under this Framework Contract (whether in tort, contract or otherwise) is no more than £1,000,000.
- 11.2 Each Party's total aggregate liability in each Contract Year under each Call-Off Contract (whether in tort, contract or otherwise) is no more than the greater of £5 million or 150% of the Estimated Yearly Charges unless specified in the Call-Off Order Form.
- 11.3 No Party is liable to the other for:
- (a) any indirect Losses; or

- (b) Loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

11.4 In spite of Clause 11.1 and 11.2, neither Party limits or excludes any of the following:

- (a) its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors;
- (b) its liability for bribery or fraud or fraudulent misrepresentation by it or its employees;
- (c) any liability that cannot be excluded or limited by Law;
- (d) its obligation to pay the required Management Charge or Default Management Charge.

11.5 In spite of Clauses 11.1 and 11.2, the Supplier does not limit or exclude its liability for any indemnity given under Clauses 7.5, 8.3(b), 9.5, 31.3 or Call-Off Schedule 2 (Staff Transfer) of a Contract.

11.6 In spite of Clauses 11.1, 11.2 but subject to Clauses 11.3 and 11.4, the Supplier's aggregate liability in each and any Contract Year under each Contract under Clause 14.8 shall in no event exceed the Data Protection Liability Cap.

11.7 Each Party must use all reasonable endeavours to mitigate any Loss or damage which it suffers under or in connection with each Contract, including any indemnities.

11.8 When calculating the Supplier's liability under Clause 11.1 or 11.2 the following items will not be taken into consideration:

- (a) Deductions; and
- (b) any items specified in Clauses 11.5 or 11.6.

11.9 If more than one Supplier is party to a Contract, each Supplier Party is jointly and severally liable for their obligations under that Contract.

12. Obeying the law

12.1 The Supplier must use reasonable endeavours to comply with the provisions of Joint Schedule 5 (Corporate Social Responsibility).

12.2 To the extent that it arises as a result of a Default by the Supplier, the Supplier indemnifies the Relevant Authority against any fine or penalty incurred by the Relevant Authority pursuant to Law and any costs incurred by the Relevant Authority in defending any proceedings which result in such fine or penalty.

12.3 The Supplier must appoint a Compliance Officer who must be responsible for ensuring that the Supplier complies with Law, Clause 12.1 and Clauses 27 to 32.

13. Insurance

- 13.1 The Supplier must, at its own cost, obtain and maintain the Required Insurances in Joint Schedule 3 (Insurance Requirements) and any Additional Insurances in the Order Form.

14. Data protection

- 14.1 The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with Joint Schedule 11 (Processing Data).
- 14.2 The Supplier must not remove any ownership or security notices in or relating to the Government Data.
- 14.3 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every 6 Months.
- 14.4 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the Security Policy and any applicable Security Management Plan.
- 14.5 If at any time the Supplier suspects or has reason to believe that the Government Data provided under a Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Relevant Authority and immediately suggest remedial action.
- 14.6 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Relevant Authority may either or both:
- (a) tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Relevant Authority receives notice, or the Supplier finds out about the issue, whichever is earlier; and/or
 - (b) restore the Government Data itself or using a third party.
- 14.7 The Supplier must pay each Party's reasonable costs of complying with Clause 14.6 unless CCS or the Buyer is at fault.
- 14.8 The Supplier:
- (a) must provide the Relevant Authority with all Government Data in an agreed open format within 10 Working Days of a written request;
 - (b) must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;
 - (c) must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice;
 - (d) securely erase all Government Data and any copies it holds when asked to do so by CCS or the Buyer unless required by Law to retain it; and
 - (e) indemnifies CCS and each Buyer against any and all Losses incurred if the Supplier breaches

Clause 14 and any Data Protection Legislation.

15. What you must keep confidential

15.1 Each Party must:

- (a) keep all Confidential Information it receives confidential and secure;
- (b) except as expressly set out in the Contract at Clauses 15.2 to 15.4 or elsewhere in the Contract, not disclose, use or exploit the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent; and
- (c) immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

15.2 In spite of Clause 15.1, a Party may disclose Confidential Information which it receives from the Disclosing Party in any of the following instances:

- (a) where disclosure is required by applicable Law or by a court with the relevant jurisdiction if, to the extent not prohibited by Law, the Recipient Party notifies the Disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;
- (b) if the Recipient Party already had the information without obligation of confidentiality before it was disclosed by the Disclosing Party;
- (c) if the information was given to it by a third party without obligation of confidentiality;
- (d) if the information was in the public domain at the time of the disclosure;
- (e) if the information was independently developed without access to the Disclosing Party's Confidential Information;
- (f) on a confidential basis, to its auditors;
- (g) on a confidential basis, to its professional advisers on a need-to-know basis; or
- (h) to the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

15.3 In spite of Clause 15.1, the Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier Staff must enter into a direct confidentiality agreement with the Relevant Authority at its request.

15.4 In spite of Clause 15.1, CCS or the Buyer may disclose Confidential Information in any of the following cases:

- (a) on a confidential basis to the employees, agents, consultants and contractors of CCS or the Buyer;
- (b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that CCS or the Buyer transfers or proposes to transfer all or any part of its business to;
- (c) if CCS or the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry

- out its public functions;
- (d) where requested by Parliament; or
- (e) under Clauses 4.7 and 16.

15.5 For the purposes of Clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in Clause 15.

15.6 Transparency Information is not Confidential Information.

15.7 The Supplier must not make any press announcement or publicise the Contracts or any part of them in any way, without the prior written consent of the Relevant Authority and must take all reasonable steps to ensure that Supplier Staff do not either.

16. When you can share information

16.1 The Supplier must tell the Relevant Authority within 48 hours if it receives a Request For Information.

16.2 Within five (5) Working Days of the Buyer's request the Supplier must give CCS and each Buyer full co-operation and information needed so the Buyer can:

- (a) publish the Transparency Information;
- (b) comply with any Freedom of Information Act (FOIA) request; and/or
- (c) comply with any Environmental Information Regulations (EIR) request.

16.3 The Relevant Authority may talk to the Supplier to help it decide whether to publish information under Clause 16. However, the extent, content and format of the disclosure is the Relevant Authority's decision in its absolute discretion.

17. Invalid parts of the contract

17.1 If any part of a Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Contract as much as required and rendered ineffective as far as possible without affecting the rest of the Contract, whether it is valid or enforceable.

18. No other terms apply

18.1 The provisions incorporated into each Contract are the entire agreement between the Parties. The Contract replaces all previous statements, agreements and any course of dealings made between the Parties, whether written or oral, in relation to its subject matter. No other provisions apply.

19. Other people's rights in a contract

19.1 No third parties may use the Contracts (Rights of Third Parties) Act 1999 (CRTPA) to enforce

any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

20. Circumstances beyond your control

- 20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under a Contract while the inability to perform continues, if it both:
- (a) provides a Force Majeure Notice to the other Party; and
 - (b) uses all reasonable measures practical to reduce the impact of the Force Majeure Event.
- 20.2 Either Party can partially or fully terminate the affected Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.

21. Relationships created by the contract

- 21.1 No Contract creates a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

22. Giving up contract rights

- 22.1 A partial or full waiver or relaxation of the terms of a Contract is only valid if it is stated to be a waiver in writing to the other Party.

23. Transferring responsibilities

- 23.1 The Supplier cannot assign, novate or transfer a Contract or any part of a Contract without the Relevant Authority's written consent.
- 23.2 The Relevant Authority can assign, novate or transfer its Contract or any part of it to any Central Government Body, public or private sector body which performs the functions of the Relevant Authority.
- 23.3 When CCS or the Buyer uses its rights under Clause 23.2 the Supplier must enter into a novation agreement in the form that CCS or the Buyer specifies.
- 23.4 The Supplier can terminate a Contract novated under Clause 23.2 to a private sector body that is experiencing an Insolvency Event.
- 23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.
- 23.6 If CCS or the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of Subcontractors at all levels of the supply chain including:
- (a) their name;

- (b) the scope of their appointment; and
- (c) the duration of their appointment.

24. Changing the contract

- 24.1 Either Party can request a Variation which is only effective if agreed in writing and signed by both Parties.
- 24.2 The Supplier must provide an Impact Assessment either:
- (a) with the Variation Form, where the Supplier requests the Variation; or
 - (b) within the time limits included in a Variation Form requested by CCS or the Buyer.
- 24.3 If the Variation cannot be agreed or resolved by the Parties, CCS or the Buyer can either:
- (a) agree that the Contract continues without the Variation; or
 - (b) terminate the affected Contract, unless in the case of a Call-Off Contract, the Supplier has already provided part or all of the provision of the Deliverables, or where the Supplier can show evidence of substantial work being carried out to provide them; or
 - (c) refer the Dispute to be resolved using Clause 34 (Resolving Disputes).
- 24.4 CCS and the Buyer are not required to accept a Variation request made by the Supplier.
- 24.5 If there is a General Change in Law, the Supplier must bear the risk of the change and is not entitled to ask for an increase to the Framework Prices or the Charges.
- 24.6 If there is a Specific Change in Law or one is likely to happen during the Contract Period the Supplier must give CCS and the Buyer notice of the likely effects of the changes as soon as reasonably practical. They must also say if they think any Variation is needed either to the Deliverables, Framework Prices or a Contract and provide evidence:
- (a) that the Supplier has kept costs as low as possible, including in Subcontractor costs; and
 - (b) of how it has affected the Supplier's costs.
- 24.7 Any change in the Framework Prices or relief from the Supplier's obligations because of a Specific Change in Law must be implemented using Clauses 24.1 to 24.4.
- 24.8 For 101(5) of the Regulations, if the Court declares any Variation ineffective, the Parties agree that their mutual rights and obligations will be regulated by the terms of the Contract as they existed immediately prior to that Variation and as if the Parties had never entered into that Variation.

25. How to communicate about the contract

- 25.1 All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they are delivered before 5:00pm on a Working Day. Otherwise the

notice is effective on the next Working Day. An email is effective at 9:00am on the first Working Day after sending unless an error message is received.

- 25.2 Notices to CCS must be sent to the CCS Authorised Representative's address or email address in the Framework Award Form.
- 25.3 Notices to the Buyer must be sent to the Buyer Authorised Representative's address or email address in the Order Form.
- 25.4 This Clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

26. Dealing with claims

- 26.1 If a Beneficiary is notified of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days.
- 26.2 At the Indemnifier's cost the Beneficiary must both:
 - (a) allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim; and
 - (b) give the Indemnifier reasonable assistance with the claim if requested.
- 26.3 The Beneficiary must not make admissions about the Claim without the prior written consent of the Indemnifier which can not be unreasonably withheld or delayed.
- 26.4 The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that does not damage the Beneficiary's reputation.
- 26.5 The Indemnifier must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.
- 26.6 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.
- 26.7 If the Indemnifier pays the Beneficiary money under an indemnity and the Beneficiary later recovers money which is directly related to the Claim, the Beneficiary must immediately repay the Indemnifier the lesser of either:
 - (a) the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money; or
 - (b) the amount the Indemnifier paid the Beneficiary for the Claim.

27. Preventing fraud, bribery and corruption

- 27.1 The Supplier must not during any Contract Period:

- (a) commit a Prohibited Act or any other criminal offence in the Regulations 57(1) and 57(2); or
- (b) do or allow anything which would cause CCS or the Buyer, including any of their employees, consultants, contractors, Subcontractors or agents to breach any of the Relevant Requirements or incur any liability under them.

27.2 The Supplier must during the Contract Period:

- (a) create, maintain and enforce adequate policies and procedures to ensure it complies with the Relevant Requirements to prevent a Prohibited Act and require its Subcontractors to do the same;
- (b) keep full records to show it has complied with its obligations under Clause 27 and give copies to CCS or the Buyer on request; and
- (c) if required by the Relevant Authority, within 20 Working Days of the Start Date of the relevant Contract, and then annually, certify in writing to the Relevant Authority, that they have complied with Clause 27, including compliance of Supplier Staff, and provide reasonable supporting evidence of this on request, including its policies and procedures.

27.3 The Supplier must immediately notify CCS and the Buyer if it becomes aware of any breach of Clauses 27.1 or 27.2 or has any reason to think that it, or any of the Supplier Staff, has either:

- (a) been investigated or prosecuted for an alleged Prohibited Act;
- (b) been debarred, suspended, proposed for suspension or debarment, or is otherwise ineligible to take part in procurement programmes or contracts because of a Prohibited Act by any government department or agency;
- (c) received a request or demand for any undue financial or other advantage of any kind related to a Contract; or
- (d) suspected that any person or Party directly or indirectly related to a Contract has committed or attempted to commit a Prohibited Act.

27.4 If the Supplier notifies CCS or the Buyer as required by Clause 27.3, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

27.5 In any notice the Supplier gives under Clause 27.3 it must specify the:

- (a) Prohibited Act;
- (b) identity of the Party who it thinks has committed the Prohibited Act; and
- (c) action it has decided to take.

28. Equality, diversity and human rights

28.1 The Supplier must follow all applicable equality Law when they perform their obligations under the Contract, including:

- (a) protections against discrimination on the grounds of race, sex, gender reassignment, religion

- (b) or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and any other requirements and instructions which CCS or the Buyer reasonably imposes related to equality Law.

28.2 The Supplier must take all necessary steps, and inform CCS or the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on a Contract.

29. Health and safety

29.1 The Supplier must perform its obligations meeting the requirements of:

- (a) all applicable Law regarding health and safety; and
- (b) the Buyer's current health and safety policy while at the Buyer's Premises, as provided to the Supplier.

29.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they are aware of at the Buyer Premises that relate to the performance of a Contract.

30. Environment

30.1 When working on Site the Supplier must perform its obligations under the Buyer's current Environmental Policy, which the Buyer must provide.

30.2 The Supplier must ensure that Supplier Staff are aware of the Buyer's Environmental Policy.

31. Tax

31.1 The Supplier must not breach any Tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. CCS and the Buyer cannot terminate a Contract where the Supplier has not paid a minor Tax or social security contribution.

31.2 Where the Charges payable under a Contract with the Buyer are or are likely to exceed £5 million at any point during the relevant Contract Period, and an Occasion of Tax Non-Compliance occurs, the Supplier must notify CCS and the Buyer of it within 5 Working Days including:

- (a) the steps that the Supplier is taking to address the Occasion of Tax Non-Compliance and any mitigating factors that it considers relevant; and
- (b) other information relating to the Occasion of Tax Non-Compliance that CCS and the Buyer may reasonably need.

31.3 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under a Call-Off Contract, the Supplier

must both:

- (a) comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions; and
- (b) indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Contract Period in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

31.4 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains the following requirements:

- (a) the Buyer may, at any time during the Contract Period, request that the Worker provides information which demonstrates they comply with Clause 31.3, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;
- (b) the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;
- (c) the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers is not good enough to demonstrate how it complies with Clause 31.3 or confirms that the Worker is not complying with those requirements; and
- (d) the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.

32. Conflict of interest

32.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential Conflict of Interest.

32.2 The Supplier must promptly notify and provide details to CCS and each Buyer if a Conflict of Interest happens or is expected to happen.

32.3 CCS and each Buyer can terminate its Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential Conflict of Interest.

33. Reporting a breach of the contract

33.1 As soon as it is aware of it the Supplier and Supplier Staff must report to CCS or the Buyer any actual or suspected breach of:

- (a) Law;
- (b) Clause 12.1; or
- (c) Clauses 27 to 32.

- 33.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in Clause 33.1 to the Buyer or a Prescribed Person.

34. Resolving disputes

- 34.1 If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.
- 34.2 If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using Clauses 34.3 to 34.5.
- 34.3 Unless the Relevant Authority refers the Dispute to arbitration using Clause 34.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:
- (a) determine the Dispute;
 - (b) grant interim remedies; and/or
 - (c) grant any other provisional or protective relief.
- 34.4 The Supplier agrees that the Relevant Authority has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.
- 34.5 The Relevant Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under Clause 34.3, unless the Relevant Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under Clause 34.4.
- 34.6 The Supplier cannot suspend the performance of a Contract during any Dispute.

35. Which law applies

- 35.1 This Contract and any Disputes arising out of, or connected to it, are governed by English law.