

Framework Schedule 6 (Order Form Template and Call-Off Schedules)
Crown Copyright 2020

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

Order Form

Pega ref CR-86987

CALL-OFF REFERENCE:	C292698
THE BUYER:	Health Research Authority
BUYER ADDRESS	2 Redman Place, Stratford, London, E20 1JQ
THE SUPPLIER:	Pegasystems Limited
SUPPLIER ADDRESS:	3rd Floor 23 Forbury Road, Reading, RG1 3JH
REGISTRATION NUMBER:	02883981
DUNS NUMBER:	576153621
SID4GOV ID:	n/a

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 28/06/2024.

It's issued under the Framework Contract with the reference number RM6194 for the provision of Back Office Software.

CALL-OFF INCORPORATED TERMS

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) RM6194
3. The following Schedules in equal order of precedence:
 - Joint Schedules for **RM6194**
 - Joint Schedule 2 (Variation Form)
 - Joint Schedule 3 (Insurance Requirements)

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

Crown Copyright 2020

- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 7 (Financial Difficulties)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)
- Call-Off Schedules for **RM6194**
 - Call-Off Schedule 1 (Transparency Reports)
 - Call-Off Schedule 3 (Continuous Improvement)
 - Call-Off Schedule 7 (Key Supplier Staff)
 - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
 - Call-Off Schedule 9 (Security)
 - Call-Off Schedule 10 (Exit Management)
 - Call-Off Schedule 14 (Service Levels)
 - Call-Off Schedule 15 (Call-Off Contract Management)
 - Call-Off Schedule 20 (Call-Off Specification)
 - Call-Off Schedule 23 (Supplier-Furnished Terms)

4. CCS Core Terms (version 3.0.10), as amended and attached as Appendix 1.

5. Joint Schedule 5 (Corporate Social Responsibility) RM6194

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:

Supplier Furnished Terms and Core Terms as amended in Appendix 1

The parties agree that:

The call-off provisions relating to TUPE under Call Off Schedule 2 (Staff Transfer) are not applicable to this agreement.

CALL-OFF START DATE: 28/06/2024.

CALL-OFF EXPIRY DATE: 27/06/2025.

CALL-OFF INITIAL PERIOD: One year

EXTENSION TO THE CONTRACT TERM

The Buyer may extend the Contract by up to 12 Months at a time, by giving not less than 30 Working Days' notice in writing to the Supplier prior to the Expiry Date, up to an additional maximum of 4 years extension.

The terms and conditions of the Contract shall apply throughout any such extended period. Extensions to be mutually agreed in writing.

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

Crown Copyright 2020

CALL-OFF DELIVERABLES

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

MAXIMUM LIABILITY

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

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **£380,452**

CALL-OFF CHARGES

“REDACTION, under FOIA Section 43 Commercial Interests”

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

Crown Copyright 2020

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices)

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

Annually in advance. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice, which contains a PO number provided to the Supplier by the Buyer.

BUYER'S INVOICE ADDRESS:

Hardcopy invoices may be sent to:

Health Research Authority
T71 PAYABLES F275
PO Box 312
LEEDS
LS11 1HP

However, electronic invoices are preferred. As our service is provided by NHS SBS the Supplier can contact NHS SBS for a Tradeshift account which will allow them to submit e-invoices to that account, but this needs to be established via NHS SBS. Further details can be found here: <https://www.sbs.nhs.uk/supplier-invoicing>

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

Crown Copyright 2020

PLEASE DO NOT SEND BOTH HARDCOPY AND ELECTRONIC INVOICES AS THIS WILL CREATE DUPLICATE INVOICES IN THE SYSTEM.

BUYER'S AUTHORISED REPRESENTATIVE

"REDACTION, under FOIA Section 40 Personal Information"

BUYER'S ENVIRONMENTAL POLICY

HRA environmental sustainability strategy – making environmental sustainability the norm - Health Research Authority

BUYER'S SECURITY POLICY

The Buyer requires that the Supplier follow the NCSC Cloud Security Principles, as detailed in Call-Off Schedule 20 (Specification) and Schedule 9 (Security).

SUPPLIER'S AUTHORISED REPRESENTATIVE

"REDACTION, under FOIA Section 40 Personal Information"

SUPPLIER'S CONTRACT MANAGER

"REDACTION, under FOIA Section 40 Personal Information"

PROGRESS REPORT FREQUENCY

As detailed in Call-Off Schedule 14 (Service Levels)

PROGRESS MEETING FREQUENCY

Operational Boards shall take place monthly as per Call Off Schedule 15 (Call Off Contract Management)

KEY STAFF

"REDACTION, under FOIA Section 40 Personal Information"

KEY SUBCONTRACTOR(S)

Framework Schedule 6 (Order Form Template and Call-Off Schedules)
Crown Copyright 2020

Not applicable

Amazon Web Services are a sub-processor. Deployment region: AWS UK, per Schedule 11 (Processing Data).

COMMERCIALLY SENSITIVE INFORMATION
As detailed in Joint Schedule 4 (Commercially Sensitive Information)

SERVICE CREDITS
As detailed in Call-Off Schedule 14 (Service Levels)

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT
The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in it's service offering and detailed in Call-Off Schedule 14 (Service Levels)

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:	"REDACTION, under FOIA Section 40 Personal Information"	Signature:	"REDACTION, under FOIA Section 40 Personal Information"
Name:	"REDACTION, under FOIA Section 40 Personal Information"	Names:	"REDACTION, under FOIA Section 40 Personal Information"
Role:	VP, Chief Business Officer & Associate GC	Role:	Chief Executive Deputy Chief Executive and Director of resources
Date:	21 June 2024 16:34 BST	Date:	24 June 2024 17:21 BST

Joint Schedule 1 (Definitions)

Crown Copyright 2020

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 Crown 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; and
 - 1.3.12 where the Buyer is a Crown Body it shall be treated as contracting with the Crown as a whole.

Joint Schedule 1 (Definitions)

Crown Copyright 2020

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;
"Application Support"	a wide variety of application services, processes and methodologies for maintaining, enhancing, managing and supporting custom or enterprise applications, packaged software applications, or network-delivered applications.
"Approval"	the prior written consent of the Buyer and "Approve" and "Approved" shall be construed accordingly;
"Audit"	<p>the Relevant Authority's right to:</p> <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 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;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

	<p>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;</p> <p>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;</p> <p>h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract;</p> <p>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;</p> <p>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</p> <p>k) verify the accuracy and completeness of any Management Information delivered or required by the Framework Contract;</p>
"Auditor"	<p>a) the Buyer's internal and external auditors;</p> <p>b) the Buyer's statutory or regulatory auditors;</p> <p>c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office;</p> <p>d) HM Treasury or the Cabinet Office;</p> <p>e) any party formally appointed by the Buyer to carry out audit or similar review functions; and</p> <p>f) successors or assigns of any of the above;</p>
"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;
"Balanced Scorecard"	a tool for Call-Off Contract management activity, through measurement of a Supplier's performance against key performance indicator, which the Buyer and Supplier may agree at the Call-Off Contract Start Date;
"Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Contract;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"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 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 up to a maximum of the number of years in total 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 Procedure and Award Criteria);
"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;
"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);
"Cap"	the maximum amount to be paid by the Buyer under a Time and Materials mechanism for the delivery of an agreed scope;
"Capped Time and Materials"	Time and Materials payable up to a specified Cap for delivery of the agreed scope of Deliverables;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"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"	<p>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:</p> <ul style="list-style-type: none"> 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 "confidential") or which ought reasonably to be considered to be confidential;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"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;
"Contracts Finder"	the Government's publishing portal for public sector procurement opportunities;
"Contract Period"	the term of either a Framework Contract or Call-Off Contract from the earlier of the: e) applicable Start Date; or f) the Effective Date until 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 GDPR;
"Core Terms"	CCS' standard terms and conditions for common goods and services which govern how Supplier 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: g) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Man 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 2020

	<p>h) 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>i) 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>j) 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>k) Overhead;</p> <p>l) financing or similar costs;</p> <p>m) 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>n) taxation;</p> <p>o) fines and penalties;</p> <p>p) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and</p> <p>q) non-cash items (including depreciation, amortisation, impairments and movements in provisions);</p>
"Crown Body"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"CRTPA"	the Contract Rights of Third Parties Act 1999;
"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 GDPR, the LED and any applicable national implementing Laws 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 2020

"Data Protection Officer"	has the meaning given to it in the GDPR;
"Data Subject"	has the meaning given to it in the 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 the 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;
"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) for the period specified in the Order Form (for the purposes of this definition the "Disaster Period");
"Disclosing Party"	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"Dispute"	any claim, dispute or difference arises 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"	<p>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:</p> <p>r) 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>s) is required by the Supplier in order to provide the Deliverables; and/or</p> <p>t) 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;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"End Date"	the earlier of: u) the Expiry Date (as extended by any Extension Period exercised by the Authority under Clause 10.2); or v) if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract;
"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;
"Estimated Year 1 Charges"	the anticipated total Charges payable by the Buyer in the first Contract Year specified in the Order Form;

"Estimated Yearly Charges"	means for the purposes of calculating each Party's annual liability under clause 11.2 : 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;
-----------------------------------	---

"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;
"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;
"Fixed Price"	the pricing mechanism whereby the Buyer agrees to pay the Supplier based on a capped price which shall cover all work performed and Deliverables required to be provided by the Supplier Staff and all materials used in the project, no matter how much work is required to complete each identified Deliverable within the agreed scope;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"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, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from:</p> <ul style="list-style-type: none"> a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under a Contract; b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; c) acts of a Crown Body, local government or regulatory bodies; d) fire, flood or any disaster; or e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available but excluding: <ul style="list-style-type: none"> i) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain; ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and iii) any failure of delay caused by a lack of funds;
"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;
"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 OJEU Notice;
"Framework Contract Period"	the period from the Framework Start Date until the End Date or earlier termination of the Framework Contract;
"Framework Expiry Date"	the 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;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"Framework Initial Period"	the initial term of the Framework Contract as specified in the Framework Award Form;
"Framework Optional Extension Period"	such period or periods beyond which the Framework Initial Period may be extended up to a maximum of the number of years in total 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 Response);
"Further Competition Procedure"	the further competition procedure described in Framework Schedule 7 (Call-Off Procedure and Award Criteria);
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679);
"General Anti-Abuse Rule"	f) the legislation in Part 5 of the Finance Act 2013 and; and g) 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 taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"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 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

Joint Schedule 1 (Definitions)

Crown Copyright 2020

	<p>electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which:</p> <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;
"Government Procurement Card"	<p>the Government's preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/government-procurement-card--2;</p>
"Guarantor"	<p>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;</p>
"Halifax Abuse Principle"	<p>the principle explained in the CJEU Case C-255/02 Halifax and others;</p>
"HMRC"	<p>Her Majesty's Revenue and Customs;</p>
"ICT Policy"	<p>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;</p>
"Impact Assessment"	<p>an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:</p> <ul style="list-style-type: none"> h) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract; i) details of the cost of implementing the proposed Variation; j) 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; k) a timetable for the implementation, together with any proposals for the testing of the Variation; and l) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;
"Implementation Plan"	<p>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;</p>
"Incremental Fixed Price"	<p>the pricing mechanism where the overall Statement of Work is based on Capped Time and Materials, but where the prices for individual Deliverables Increments are fixed prior to the work being undertaken. The Charges for the first Deliverable Increment or Deliverables Increments for the Statement of Work will be fixed, but the Charges for subsequent Deliverables Increments will be</p>

Joint Schedule 1 (Definitions)

Crown Copyright 2020

	reviewed and refined prior to the execution of each subsequent Deliverables Increment within the same Statement of Work;
"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>m) in respect of a person:</p> <p>n) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or</p> <p>o) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or</p> <p>p) a petition is presented for its winding up (which is not dismissed within fourteen (14) Working Days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or</p> <p>q) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or</p> <p>r) an application is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or</p> <p>s) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or</p> <p>t) being a "small company" within the meaning of section 382(3) of the Companies Act 2006, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or</p>

Joint Schedule 1 (Definitions)

Crown Copyright 2020

	<p>u) where the person is an individual or partnership, any event analogous to those listed in limbs (a) to (g) (inclusive) occurs in relation to that individual or partnership; or</p> <p>v) any event analogous to those listed in limbs (a) to (h) (inclusive) occurs under the law of any other jurisdiction;</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>w) 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>x) 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>y) 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;
"IR35"	the off-payroll rules requiring individuals who work through their company pay the same 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 ;
"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;
"Joint Control"	where two or more Controllers agree to jointly determine the purposes and means of Processing Personal Data;
"Key Personnel"	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;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

	<p>z) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or</p> <p>aa) 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</p> <p>bb) 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,</p> <p>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;</p>
"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;
"KPI Target"	a key performance indicator target included in the Balanced Scorecard;
"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;
"LED"	Law Enforcement Directive (Directive (EU) 2016/680);
"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;
"Man Day"	7.5 Man Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day;
"Man 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;
"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);

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"Management Information" or "MI"	the management information specified in Framework Schedule 5 (Management Charges and Information);
"Marketing Contact"	shall be the person identified in the Framework Award Form;
"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"> cc) contains any material errors or material omissions or a missing mandatory field; or dd) is submitted using an incorrect MI reporting Template; or ee) 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 National Insurance Contributions Regulations 2012 (SI 2012/1868) made under section 132A of the Social Security Administration Act 1992;
"New IPR"	<ul style="list-style-type: none"> ff) 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 gg) 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; but shall not include the Supplier's Existing IPR;
"Occasion of Tax Non-Compliance"	where: <ul style="list-style-type: none"> hh) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which 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 2020

	<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>ii) 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>jj) 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>kk) 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) manpower resources 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 manpower grade;</p> <p>iii) a list of Costs underpinning those rates for each manpower grade, being the agreed rate less the Supplier Profit Margin; and</p> <p>iv) Reimbursable Expenses, if allowed under the Order Form;</p> <p>ll) Overheads;</p> <p>mm) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables;</p> <p>nn) the Supplier Profit achieved over the Framework Contract Period and on an annual basis;</p> <p>oo) 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>pp) 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>qq) the actual Costs profile for each Service Period;</p>

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"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 GDPR;
"Personal Data Breach"	has the meaning given to it in the 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 GDPR;
"Processor"	has the meaning given to it in the GDPR;
"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;
"Progress Meeting"	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"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;
"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>rr) 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>ss) 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>tt) 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>uu) 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), 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.
"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;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"Recipient Party"	the Party which receives or obtains directly or indirectly Confidential Information;
"Rectification Plan"	<p>the Supplier's plan (or revised plan) to rectify it's breach using the template in Joint Schedule 10 (Rectification Plan Template) which shall include:</p> <p>vv) full details of the Default that has occurred, including a root cause analysis;</p> <p>ww) the actual or anticipated effect of the Default; and</p> <p>xx) 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 10.4.3 to 10.4.5 (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>yy) 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>zz) 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>aaa) 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>bbb) 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>

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"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 10.6 given by the Supplier to the Buyer providing notification that payment has not been received on time;
"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;
"Restricted Staff"	any person employed or engaged by either Party, in the capacity of director or in any research, technical, IT, security, engineering, procurement, financial, legal or managerial role who has been engaged in the provision of the Deliverables or management of the Contract either as principal, agent, employee, independent contractor or in any other form of employment or engagement over the previous 12 months, directly worked with or had any material dealings, but shall not include any person employed or engaged in an administrative, clerical, manual or secretarial capacity;
"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;
"Schedules"	any attachment to a Framework Contract or Call-Off Contract which contains important information specific to each aspect of buying and selling;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"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 Credits) 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;
"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: ccc) the Deliverables are (or are to be) provided; or ddd) 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;
"Software Support and Maintenance"	Software Support and Maintenance includes any software upgrades, annual updates, patches and fixes needed to improve functionality and keep the software in working order;
"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;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"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"	<p>any:</p> <p>eee) 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;</p> <p>fff) standards detailed in the specification in Schedule 1 (Specification);</p> <p>ggg) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time;</p> <p>hhh) relevant Government codes of practice and guidance applicable from time to time;</p>
"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;
"Statement of Requirements"	a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Call-Off Procedure;
"Statement of Works" "(SOW)"	the document which, upon its execution by the Buyer and Supplier, shall become incorporated into their Call-Off Contract and outlines the agreed body of works to be undertaken as part of the Call-Off Contract Deliverables. There may be any number of Statements of Work incorporated into a Call-Off Contract and each Statement of Work may include (but is not limited to) the Statement of Requirements, identified output(s), completion date(s) and charging method(s);
"SOW End Date"	the date up to and including this date when the supply of the Deliverables under the Statement of Work shall cease;
"SOW Start Date"	the date of the start of the Statement of Works as stated in the SOW;
"Standing Instructions"	Standing Instructions are a mechanism that supports the implementation of new policy that is mandated across government as a whole or in certain sectors. It is not possible at the Framework Agreement procurement stage to provide for every instance but examples such as the mandate of technical standards i.e. the use of Greening government ICT strategy; or implementation of standardisation across government.
"Storage Media"	the part of any device that is capable of storing and retrieving data;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"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 Compliance Officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
"Supplier's Confidential Information"	iii) 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; jjj) 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; kkk) 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;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"Supplier Marketing Contact"	shall be the person identified in the Framework Award Form;
"Supplier Non-Performance"	where the Supplier has failed to: III) Achieve a Milestone by its Milestone Date; mmm) provide the Goods and/or Services in accordance with the Service Levels ; and/or nnn) 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;
"Supply Chain Information Report Template"	the document at Annex 1 of Schedule 12 Supply Chain Visibility;
"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;

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"Test Issue"	any variance or non-conformity of the Deliverables or Deliverables from their requirements as set out in a Call-Off Contract;
"Test Plan"	a plan: ooo) for the Testing of the Deliverables; and ppp) setting out other agreed criteria related to the achievement of Milestones;
"Tests and Testing"	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" 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 – (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);
"Variation"	has the meaning given to it in Clause 24 (Changing the 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; and

Joint Schedule 1 (Definitions)

Crown Copyright 2020

"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.
"Work Day"	a minimum of 7.5 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 2020

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 2020

Joint Schedule 3 (Insurance Requirements)
Crown Copyright 2020

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 2020

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 2020

- 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 2020

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 five million pounds (£5,000,000);
 - 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 five million pounds (£5,000,000); and
 - 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); and
 - 1.4 product liability insurance with cover (for a single event or series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

Joint Schedule 3 (Insurance Requirements)
Crown Copyright 2020

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		Service performance related material, including but not limited to: a) Regular and ad-hoc service and reports with the exception of the mandatory minimum Cabinet Office Transparency publication requirements. b) Results of any benchmarking c) Rectification plans and material related to the conduct and/or outcome of such plans	Term + 5 years
2		Supplier Solution and Software related business know how	Term + 5 years
3		Documents produced or provided for service improvement and value for money produced by the Supplier	Term + 5 years
4		Information and documents provided which set out Suppliers insurance offering and financial standing	Term + 5 years
5		Reports, materials and data provided under any audit	Term + 5 years
6		Amounts detailed relating to compensation on termination (if any)	Term + 5 years
7		Any document or section of a document containing pricing, including but not limited to: a) Impact assessments/Change authorisation notes. b) Change Requests/amendments. Estimates, evaluation reports and proposals.	Term + 5 years

Joint Schedule 5 (Corporate Social Responsibility)

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.

3. Modern Slavery, Child Labour and Inhumane Treatment

"Modern Slavery 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.

- 3.1 The Supplier:
 - 3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;
 - 3.1.2 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;
 - 3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2020

- 3.1.4 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 offenses anywhere around the world.
- 3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offenses anywhere around the world.
- 3.1.6 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;
- 3.1.7 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;
- 3.1.8 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;
- 3.1.9 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;
- 3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;
- 3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

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;
- 4.1.3 All workers shall be 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;
- 4.1.4 not make deductions from wages:
 - (a) as a disciplinary measure

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2020

- (b) except where permitted by law; or
- (c) without expressed permission of the worker concerned;
- 4.1.5 record all disciplinary measures taken against Supplier Staff; and
- 4.1.6 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

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:
 - (a) the extent;
 - (b) frequency; and
 - (c) hours worked;

by individuals and by the Supplier Staff as a whole;

- 1.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.
- 1.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:
 - 1.3.1 this is allowed by national law;
 - 1.3.2 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
 - 1.3.3 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.
- 1.4 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.

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2020

2. Sustainability

- 2.1 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>

Joint Schedule 5 (Corporate Social Responsibility)
Crown Copyright 2020

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

Joint Schedule 7 (Financial Difficulties)**1. Definitions**

1.1 In this Schedule, 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 Annex 2 and
"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; ii) non-payment by the Monitored Company of any financial indebtedness; iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

	iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company 3 in each case which CCS 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;
"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 Annex 1.

2. When this Schedule applies

2.1 The Parties shall comply with the provisions of this Schedule 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 Schedule 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 represents to CCS 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 Annex 2.

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

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 CCS within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by CCS (such

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

requests not to exceed 4 in any Contract Year) with the most recent D&B credit check report. The Supplier shall:

3.3.1 Not used

3.3.2 promptly notify (or shall procure that its auditors promptly notify) CCS 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.

3.4 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 CCS becomes aware of the Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and CCS shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

Not Used

4.1.1 Not used

4.1.2 Not Used

4.2 The Supplier shall:

4.2.1 at the request of CCS meet CCS 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

4.2.2 where CCS 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 CCS 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

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

- (b) provide such financial information relating to the Monitored Company as CCS may reasonably require.

4.3 If CCS 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 CCS 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 CCS or referred to the Dispute Resolution Procedure.

4.4 If CCS 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.

4.5 Following Approval of the Financial Distress Service Continuity Plan by CCS, the Supplier shall:

- 4.5.1 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;
- 4.5.2 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
- 4.5.3 comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).

4.6 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 CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.4.6.

4.7 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 CCS of a Financial Distress Event in accordance with Paragraph 3.4;

Joint Schedule 7 (Financial Difficulties)

Crown Copyright 2020

- 5.1.2 CCS 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.

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

Joint Schedule 7 (Financial Difficulties)
Crown Copyright 2020

ANNEX 1: RATING AGENCIES

Experian

Joint Schedule 7 (Financial Difficulties)
Crown Copyright 2020

ANNEX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

Entity	Credit rating (long term)
Supplier	Experian Risk Level – Medium Risk

NOTE: Buyer has carried out an Experian check at the start of this contract and reflected in Annex 1. However, Parties have agreed that Annex 1 and 2 apply as at start of this contract but a Financial Distress Event under definition 2(a) 'credit rating' shall only be deemed to occur if Supplier is showing as High Risk of failure by way of a D&B report for more than 1 month and this shall be the deemed to be the Credit Rating Threshold for the purposes of this Schedule.

Joint Schedule 10 (Rectification Plan)
Crown Copyright 2020

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 2020

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 10 (Rectification Plan)

Crown Copyright 2020

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

Joint Schedule 11 (Processing Data)

Status of the Controller

1. 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. 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

2. 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.
3. The Processor shall notify the Controller with undue delay if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
4. 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;
 - (b) an assessment of the necessity and proportionality of the Processing in relation to the Services;
 - (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.
5. 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*), unless the Processor is required to do otherwise by Law. If it

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

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, for the processing of Client Personal Data in the context of providing the Supplier services in such a manner to ensure a level of security appropriate to the risk to the Client Personal Data when it is processed by the Supplier;
- (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*);
 - (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
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
- (d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained (which it has under Annex 1) and the following conditions are fulfilled:
 - (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) 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
 - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

- (e) at the written direction 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.
6. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller with undue delay if in relation to it Processing Personal Data under or in connection with the Contract it:
- (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 Personal Data Breach.
7. The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
8. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including providing without unreasonable delay:
- (a) the Controller with full details and copies of the complaint, communication or request;
 - (b) such assistance as is reasonably requested by the Controller to enable it 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 Personal Data Breach; 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.

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

9. 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 GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
 - (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
10. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
11. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
12. 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;
 - (b) obtain the written consent of the Controller;
 - (c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
 - (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

This provision is satisfied under Annex1.
13. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
14. The Relevant Authority may, at any time on not less than 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).
15. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 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

16. 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 GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (*Processing Data*).

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

Independent Controllers of Personal Data

17. 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.
18. 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.
19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 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.
20. The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
21. 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 GDPR); and
 - (c) where it has recorded it in Annex 1 (*Processing Personal Data*).
22. 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 GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.
23. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 GDPR and shall make the record available to the other Party upon reasonable request.
24. 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 provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

- (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.
25. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach 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 Personal Data Breach;
 - (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.
26. 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*).
27. 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*).
28. Notwithstanding the general application of paragraphs 2 to 15 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 Independent Controller of Personal Data in accordance with paragraphs 16 to 27 of this Joint Schedule 11.

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

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: "REDACTION, under FOIA Section 40 Personal Information"
- 1.2 The contact details of the Supplier's Data Protection Officer are: Privacy Working Group privacy@pega.com
- 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 2 to paragraph 15 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"> • <i>Names and addresses of researchers and sponsors in relation to research studies.</i> <p>The Supplier is Controller and the Relevant Authority is Processor</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 2 to paragraph 15 of the following Personal Data:</i></p> <ul style="list-style-type: none"> • <i>N/A</i> <p>The Parties are Joint Controllers</p> <p><i>The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:</i></p> <ul style="list-style-type: none"> • <i>N/A</i> <p>The Parties are Independent Controllers of Personal Data</p> <p><i>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</i></p>

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

	<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>
Duration of the Processing	<i>The duration of the contract.</i>
Nature and purposes of the Processing	<p><i>[Please be as specific as possible, but make sure that you cover all intended purposes.</i></p> <p><i>The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</i></p> <p><i>The purpose might include: employment processing, statutory obligation, recruitment assessment etc]</i></p>
Type of Personal Data	<i>Names and addresses.</i>
Categories of Data Subject	<i>Research study submitters and associated sponsors.</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	<i>Please refer to Call-Off Schedule 10 (Exit Management)</i>

Additional Notes:**1. General provisions on data**

Framework Ref: RM6194

Project Version: v1.0

Model Version: v4.0

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

Buyer will ensure that it has the necessary consents, notices and other requirements to enable lawful processing.

To the extent Data Protection Legislation applies to Pegasystems's processing of Buyer Personal Data, then the following terms apply:

- a. The parties intend that, in relation to such processing, Buyer is the controller and Pegasystems is a processor.
- b. Each party will comply with the obligations applicable to it pursuant to the Data Protection Legislation;
- c. When acting as the controller, Buyer is responsible for the processing, access and use of Buyer Personal Data, and for responding to data subjects' requests concerning their rights under the Data Protection Legislation. If Buyer is unable to respond to or fulfill such requests, Pegasystems shall assist Buyer by providing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Buyer's obligation to respond to such requests.
- d. Buyer authorizes Pegasystems to process Buyer Personal Data in order to provide the services.

2. Subprocessors and Affiliates

- a. Pegasystems may engage the services of its affiliates and subprocessors published at: <https://community.pegasystems.com/knowledgebase/articles/pegasystems-subprocessors> (the "**Website**") to provide the Pega Cloud. Pegasystems may also engage subprocessors in the course of providing professional services. Buyer consents to the use of subprocessors, including as concerns data transfers. Pegasystems shall inform Buyer by updating the Website, or by notifying Buyer in writing, of any intended changes concerning the addition or replacement of the subprocessors. Buyer will have 14 days from the date of such notice to object to the change. In the event of no objection, Buyer is deemed to have accepted the subprocessor. If Buyer objects in good faith to the appointment or replacement of a subprocessor, Buyer shall cooperate with Pegasystems in good faith in determining a replacement subprocessor. If the parties are unable to agree on a replacement subprocessor within a reasonable time period, Pegasystems or Buyer may terminate the affected Schedule(s) with immediate effect on written notice to the other party.

- b. Where Pegasystems engages the services of an affiliate or subprocessor for carrying out any part of the services or Subscription Services, it shall impose on that subprocessor substantially the same data protection obligations as set forth herein, including sufficient guarantees to implement the technical and organizational measures appropriate for their processing obligations Pegasystems is fully liable to Buyer for the performance of its subprocessors' data protection obligations.

- c. Pegasystems shall ensure that its personnel, and those of its affiliates and subprocessors, authorized to provide Subscription Services have committed themselves to appropriate obligations of confidentiality.

3. Technical and Organizational Measures

- a. Pegasystems has implemented and shall maintain appropriate technical and organizational security measures for the processing of Buyer Personal Data in the context of providing the Pegasystems services in such a manner (i) to ensure a level of security appropriate to the risk to the Buyer Personal Data when it is processed by Pegasystems and (ii) to enable Pegasystems to assist Buyer in the fulfillment of its obligations to respond to requests from data subjects exercising their rights under Data Protection Legislation.

- b. Pegasystems will not assess the content of Buyer Personal Data in order to identify information subject to specific legal requirements. Buyer is solely responsible for complying with incident notification laws applicable to Buyer and fulfilling any third-party notification obligations related to regulators and/or data subjects.

4. Data Residency and Data Transfer

Pegasystems offers geographically segmented data residency services specific to its Pega Cloud offering. If Buyer selects a regional zone in the European Union in the applicable Subscription Schedule, then Buyer Data, including all Buyer Personal Data, will be stored at a data center(s) in the European Union and will not be transferred or accessed from outside of the European Union except at the Buyer's instruction or in connection with a support request submitted by Buyer. Pegasystems may provide network monitoring and system provisioning activities for the Environments from its network operation centers located inside and outside of the European Union.

5. Network Monitoring

Without accessing the Buyer's data, Pegasystems may provide network monitoring and system provisioning activities for the Environments from its network operation centers located inside and outside of the European Union.

6. Screen Shots

Framework Ref: RM6194

Project Version: v1.0

Model Version: v4.0

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

Notwithstanding the foregoing, as part of entering and/or resolving a support request, the Buyer could incidentally transfer personal data via a shared screen, screen shot, customer log or database extract to Pegasystems' Global Customer Support organization. To the extent that personal data is transferred outside of the European Economic Area or Switzerland in connection with a support request or otherwise at the Customer's instruction, it shall only be transferred to an affiliate or subcontractor (i) established in a country which ensures an adequate level of protection, as decided by the European Commission, or (ii) if such transfer is governed by other appropriate transfer mechanisms under the Data Protection Legislation including but not limited to the use of standard data protection clauses adopted by the European Commission or adherence to the EU-US and Swiss-US Privacy Shield Frameworks.

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

Annex 2 - Joint Controller Agreement -N/A / NOT USED**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 2 (Joint Controller Agreement) in replacement of paragraphs 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 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 [Supplier/Relevant Authority]:

- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the 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 GDPR;
- (d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services 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 [Supplier's/Relevant Authority's] 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 [x] months on:

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

- (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 Services 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 Services 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 2020

- (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 2 (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;
 - (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 Personal Data Breach having taken account of the:
 - (i) nature of the data to be protected;
 - (i) harm that might result from a Personal Data Breach;
 - (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
- (i) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

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

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the Relevant Authority and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

(b) all reasonable assistance, including:

- (i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach 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 Relevant Authority to assist in the investigation, mitigation and remediation of a Personal Data Breach;
- (iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; 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 Personal Data Breach, with complete information relating to the Personal Data Breach, 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 Personal Data Breach 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 Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(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 Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

4. Audit

4.1 The Supplier shall permit:

- (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 2 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 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 Services.

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 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

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

- (a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, 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 Personal Data Breach. 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 Personal Data Breach;
- (b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach 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 Personal Data Breach; 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 Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach 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 Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. 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 Personal Data Breach (the "**Claim Losses**"):

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

- (a) if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;
- (b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
- (c) if responsibility for the relevant Personal Data Breach 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 Personal Data Breach, having regard to all the circumstances of the Personal Data Breach 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 2 (*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

10.1 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.

Joint Schedule 11 (Processing Data)

Crown Copyright 2020

Call-Off Schedule 1 (Transparency Reports)

Call-Off Ref:

Crown Copyright 2020

Call-Off Schedule 1 (Transparency Reports)

- 1.1 The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (<https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles>)). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.
- 1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.
- 1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.
- 1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

Call-Off Schedule 1 (Transparency Reports)

Call-Off Ref:

Crown Copyright 2020

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
Service Level Agreement / KPI Performance	Performance against SLAs / KPIs for the purposes of reporting to Cabinet Office under the KPI publication mandate.	As specified in Call-Off Schedule 14 (Service Levels)	As specified in Call-Off Schedule 14 (Service Levels)

Call-Off Schedule 3 (Continuous Improvement)

Call-Off Ref:

Crown Copyright 2020

Call-Off Schedule 3 (Continuous Improvement)

1. Buyer's Rights

- 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.

2. Supplier's Obligations

- 2.1 The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.
- 2.2 The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.
- 2.3 Continuous improvement will be managed as part of the Operational Board (Schedule 15). Software updates support the evolution of Pega products and provide new functionality and enhancements to these applications within the functional domain of the licensed components. Software updates are provided in accordance with the Client Support Handbook.

"Client Support Handbook" means the terms for Pegasystems' provided support, upgrades, and updates located at:
<https://docs.pega.com/supportpega-client-handbook/supportpega-client-handbook>, as may be periodically updated.

Call-Off Schedule 7 (Key Supplier Staff)
Call-Off Ref:
Crown Copyright 2020

Call-Off Schedule 7 (Key Supplier Staff)

- 1.1 The Annex 1 to this Schedule lists the key roles (“**Key Roles**”) and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.
- 1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.
- 1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.
- 1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:
 - 1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
 - 1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or
 - 1.4.3 the person’s employment or contractual arrangement with the Supplier or Subcontractor changes, or reassignment is required due to company policy, or is terminated for material breach of contract by the employee.
- 1.5 The Supplier shall:
 - 1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);
 - 1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
 - 1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff’s employment contract, this will mean at least three (3) Months’ notice;
 - 1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and

Call-Off Schedule 7 (Key Supplier Staff)

Call-Off Ref:

Crown Copyright 2020

- 1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.
- 1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

Call-Off Schedule 7 (Key Supplier Staff)
Call-Off Ref:
Crown Copyright 2020

Annex 1- Key Roles

Key Role
Account Executive

Call-Off Schedule 7 (Key Supplier Staff)
Call-Off Ref:
Crown Copyright 2020

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

Call-Off Ref:

Crown Copyright 2020

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):

"BCDR Plan"	1 has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	2 has the meaning given to it in Paragraph 2.3.2 of this Schedule;
"Disaster Recovery Deliverables"	3 the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	4 has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	5 the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	6 any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	7 has the meaning given to it in Paragraph 6.3 of this Schedule; and
"Supplier's Proposals"	8 has the meaning given to it in Paragraph 6.3 of this Schedule;

2. BCDR Plan

- 2.1 The Buyer and the Supplier recognise that, where specified in Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.
- 2.2 The Buyer recognises that in most cases the Supplier will have in place a BCDR Plan for their services which will meet industry standards and satisfy the Buyer's requirements. Where this is the case this should be provided to the Customer at the earliest opportunity. It is acknowledged that as these form part of a standard service it may not be possible for a Customer to request adjustments to the plan.

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

Call-Off Ref:

Crown Copyright 2020

- 2.3 Within 14 days of a request, the Supplier will arrange for data room set up to be provided to the Buyer so the Buyer can view a summary of the Supplier's BCDR Plan.
The BCDR Plan shall detail the processes and arrangements that the Supplier shall follow to:
- 2.3.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and
 - 2.3.2 the recovery of the Deliverables in the event of a Disaster
- 2.4 The BCDR Plan shall include a section relating to business continuity and a section relating to disaster recovery :
- 2.4.1 Not used;
 - 2.4.2 Not used;
 - 2.4.3 Not used;

3. General Principles of the BCDR Plan

- 3.1 The BCDR Plan shall:
- 3.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;
 - 3.1.2 provide details of how the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer;
 - 3.1.3 not used;
 - 3.1.4 not used;
 - 3.1.5 contain details of risk analysis, including:
- 3.2 The BCDR Plan shall be designed so as to ensure that:
- 3.2.1 the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan summary;
 - 3.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;
 - 3.2.3 it complies with the relevant provisions of ISO/IEC 27001; ISO22301 and all other industry standards from time to time in force; and
 - 3.2.4 it details a process for the management of disaster recovery testing.
- 3.3 Not used.
- 3.4 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.

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

Call-Off Ref:

Crown Copyright 2020

3.4.1

4. Review and changing the BCDR Plan

4.1 The Supplier shall review the BCDR Plan:

4.1.1 on a regular basis and as a minimum once annually

4.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked

4.2 Each review of the BCDR Plan 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 Supplier shall reasonably require.

5. Testing the BCDR Plan

5.1 The Supplier shall test the BCDR Plan:

5.1.1 regularly and in any event not less than once annually

6. Invoking the BCDR Plan

6.1 The Supplier shall immediately invoke the BCDR Plan in accordance with the BCDR Plan summary provided to the Buyer (and shall inform the Buyer promptly of such invocation if it impacts the Buyer).

7. Circumstances beyond your control

7.1 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.

NOTE: PLEASE REFER TO SUBSCRIPTION DOCUMENTATION RELATING TO INCIDENT REPORTING AND DATA RECOVERY.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2020

Call-Off Schedule 9 (Security)

SECURITY STANDARDS

In addition to Supplier maintaining Cyber Essentials, the following shall also apply:

1. **Security Practices & Review**

1.1. Pegasystems shall maintain an information and physical security program for the protection of Client personal information and confidential information in environments and on equipment controlled by Pegasystems (the "**Pegasystems Security Program**").

1.2. As part of the Pegasystems Security Program, Pegasystems conducts periodic reviews of security practices against various leading industry standards, such as NIST, ISO 27001 and SSAE18 SOC2. Pegasystems regularly re-evaluates and updates the Pegasystems Security Program as the industry evolves, new technologies emerge, or new threats are identified. Upon request, Pega will maintain and make available on at least an annual basis, a reasonable information security questionnaire completed with answers concerning Pegasystems Security Program specific to the services provided under the applicable Schedule.

1.3. The Pegasystems Security Program consists of the following:

a. **Physical Access**

1. Pegasystems maintains physical security standards designed to prohibit unauthorized physical access to Pegasystems facilities and equipment. This is accomplished by the following practices:

- physical access to locations is limited to Pegasystems employees, subcontractors and authorized visitors;
- Pegasystems employees, subcontractors and authorized visitors are issued identification cards that must be worn while on premises;
- monitoring access to Pegasystems facilities, including restricted areas and equipment within Pegasystems facilities;
- all access to the data centers where client personal data is hosted is logged, monitored, and tracked; and
- data centers are secured with alarm systems and video cameras.

b. **Access Control and Administration**

2. Pegasystems maintains the following standards for access control and administration of the in environments and on equipment controlled by Pegasystems or Pegasystems contractors.

- administrator accounts are only be used for the purpose of performing administrative activities;

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2020

- each account with administrative privileges must be traceable to a uniquely-identifiable individual;
- all access to computers and servers must be authenticated and within the scope of an employee's job function;
- initial passwords must be changed by the user on first use;
- the display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them;
- passwords must be uniquely identifiable to an individual;
- passwords must be encrypted when transmitted or stored;
- password complexity should never be less than three (3) out of four (4) character classes and must have character class choices such as upper-case letters, lower case letters, numeric digits, or special characters;
- passwords must not contain three (3) or more identical consecutive characters;
- password length must be configured to be at least twelve (12) characters;
- passwords shall expire between ninety (90) and one hundred eighty (180) days depending on its length; twelve (12) characters – ninety (90) days, sixteen (16) characters – one hundred thirty-five (135) days, twenty plus (20+) characters – one hundred eighty (180) days;
- automatic time-out of access to computers and servers if left idle with the requirement for password authentication for re-access; and
- per Pega policy, accounts must be set to lockout after six (6) erroneous failed login attempts.

c. Virus Scanning and Logging

- Computers and servers have commercially reasonable up-to-date versions of system security software which may include host firewall, anti-virus protection and up-to-date patches and virus definitions. Such software is configured to scan for and promptly remove or fix identified findings.
- Pegasystems maintains logs of various components of the infrastructure and an intrusion detection system to monitor, detect, and report misuse patterns, suspicious activities, unauthorized users, and other actual and threatened security risks.

d. Encryption

- Pega encrypts all data in transit over public networks.
- Data originating from or residing within Pega networks is encrypted at rest.

2. Pegasystems Personnel

- 2.1. Employees and contractors are required by policy to be trained on Pegasystems' privacy and security policies and made aware of their responsibilities regarding privacy and security practices.
- 3.
- 2.2. Pegasystems employees and contractors are contractually bound to maintain the confidence of Client personal information or confidential information and comply with applicable Pegasystems policies, standards or requirements in relation to the processing of Client personal information. Failure to comply with those policies, standards or requirements will be subject to investigation which may result in disciplinary action up to and including termination of employment or engagement by Pegasystems and legal action as appropriate.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2020

3. **Security Breach Notification and Security Incident Management**

- 3.1. Pegasystems will notify Client within twenty-four (24) hours of becoming aware of a Security Incident. A “**Security Incident**” means the unauthorized access to or use of Client information on environments or equipment controlled by Pegasystems affecting the confidentiality, availability and integrity of such Client confidential information. Pegasystems will provide Client with updates on the status of the Security Incident until the matter has been remediated. The reports will include, without limitation, a description of the Security Incident, actions taken and remediation plans.
- Notice of a Security Incident shall be sent via email to the security contacts that Client designates in its Pega Support Portal (found here: <https://msp.pegacom>).
 - Similarly, if Client becomes aware of a Security Incident that affects the Services, Client shall, without undue delay, notify Pegasystems of such and inform Pegasystems of the scope of the Security Incident. Such notice from Client to Pegasystems should be provided to: SecurityBreachNotice@pegacom and/or 1-617-866-6800.
- 3.2 Proportionate to acts or omissions of Pegasystems resulting in a Security Incident, and subject to terms and limitations set forth in the Agreement, Pegasystems agrees to pay reasonable costs for: (i) required notice to individuals affected by the Security Incident; and (ii) credit monitoring service for twelve (12) months for affected data subjects, except to the extent applicable law specifies a longer period for applicable credit monitoring services, in which case such longer period shall then apply.
- 3.3 Pegasystems will, at the request and cost of the Client:
- Provide reasonable assistance to the Client in notifying a Security Incident to the supervisory authority competent under the privacy laws applicable to the Client; and
 - Provide reasonable assistance to the Client in communicating a Security Incident to data subjects in cases where the Security Incident is likely to result in a high risk to the rights and freedoms of individuals.

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

Crown Copyright 2020

Call-Off Schedule 10 (Exit Management)

1. The following exit arrangements shall apply:

1.1 At the end of this Call-Off Contract (upon Ending or expiry); Supplier will make the Buyer's data in its possession available to the Buyer by means of a backup file of the Production Environment database and that is encrypted to customary standards, unless otherwise agreed in writing, at no cost to the Buyer.

1.2 The Buyer shall request any such information prior to the Ending of the Call-Off Contract.

1.3 Upon providing the Buyer data to the Buyer, or the lapse of the time period for Buyer to request its data, Pegasystems will have no obligation to maintain or provide the Buyer's data in its possession or control and may delete such Buyer data, unless legally prohibited.

2. Other than contained within clause 1 above, there is no other offboarding plan for this Call-Off Contract.

2.1 The parties may discuss any additional offboarding requirements over and above those contained within clause 1 above, and any associated costs, timescales and resources, prior to the expiry of this Call-Off Contract.

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2020

Call-Off Schedule 14 (Service Levels)**1. Definitions**

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

"Critical Service Level Failure"	has the meaning given to it in the Order Form;
"Service Credits"	1 any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
"Service Credit Cap"	2 has the meaning given to it in the Order Form;
"Service Level Failure"	3 means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	4 shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
"Service Level Threshold"	5 shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

2. What happens if you don't meet the Service Levels

- 2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.
- 2.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Performance Measure. For clarification, Service Credit is only applicable to Uptime SLA.
- 2.3 No monthly reports are automatically provided by the Supplier. Availability is published at <https://status.pegasys.net> and service response times are recorded in Service Tickets. The Supplier shall send a

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2020

Performance Monitoring Report for the previous month to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule following a written request from the Buyer to the Global Service Center if the Buyer reasonably believes a Service Level Failure has occurred.

- 2.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure.

(a)

Part A: Service Levels and Service Credits

1. Service Levels

If the Supplier is in material Default the Buyer, in its absolute discretion and without limiting any other of its rights, may:

- 1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;
- 1.2.2 instruct the Supplier to provide and comply with a mutually agreed Rectification Plan Process;
- 1.2.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or

2. Service Credits

- 2.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period, provided that, Supplier shall only be required to provide a report following a written request made by the Buyer if Buyer reasonably believes the Service level has not been met. Where no written request has been made by the Buyer because it has not experienced any reduction of service, then Buyer is permitted to report a Service Level of Good Target.
- 2.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2020

Annex A to Part A: Services Levels and Service Credits Table

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
Monthly Uptime %	Uptime	99.95%	<p>Good target: $\geq 99.95\%$</p> <p>Approaching target: 99% - 99.94%</p> <p>Requires Improvement target: 98% - 98.9%</p> <p>Inadequate target: $\leq 97.9\%$</p>	<p>The Buyer is required to claim 'Service Credits' in writing within 30 days of the preceding month.</p> <p>"Service Level Agreement" means the Pega Cloud Production Environment availability of 99.95% Monthly Uptime Percentage as described at the following link: https://docs.pega.com/pega-cloud-services-subscription-documentation/service-level-agreement-pega-cloud-services.</p> <p>The Service Credit is linked to SaaS fees and not professional services fees. The service credit calculation is located at the above link.</p>

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2020

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
Security Incident Reporting	Timelines	100%	<p>Good target: 100%</p> <p>Approaching target: 99-98%</p> <p>Requires Improvement target: 97-96%</p> <p>Inadequate target: 95% or below</p>	No Service Credit applicable. The Supplier will notify the Buyer within twenty-four (24) hours of becoming aware of a Security Incident. A "Security Incident" means the unauthorised access to or use of Buyer information on environments or equipment controlled by the Supplier affecting the confidentiality, availability and integrity of such Buyer confidential information
Service Desk Response Time (Severity 1)	Timelines:	100% for Sev 1	<p>Good target: 100%</p> <p>Inadequate target: <100%</p>	<p>No Service Credits. Response times are detailed in Client Support Handbook.</p> <p>Support: 24 Hours, 7 days a week.</p> <p>Response Time: Direct Communication within 15 minutes.</p> <p>Updates: At a minimum, every eight hours or mutually agreed upon frequency.</p>
Service Desk Response Time (Severity 2)	Timelines:	100% for Sev 2	<p>Good target: 100%</p> <p>Approaching target: 90-94%</p> <p>Requires Improvement target: 85-89%</p> <p>Inadequate target: Below 89%</p>	<p>No Service Credits. Response times are detailed in Client Support Handbook.</p> <p>Support: 5 days a week, standard business hours</p> <p>Response Time: Direct Communication within 1 business hour.</p> <p>Updates: At a minimum 1 business day or mutually agreed upon frequency.</p>

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2020

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
Service Desk Response Time (Severity 3)	Timelines:	100% for Sev 3 and 95% for other lower Sevs.	<p>Good target: 100% for Sev 1 and 95 % for other Sevs.</p> <p>Approaching target: 90-94%</p> <p>Requires Improvement target: 85-89%</p> <p>Inadequate target: Below 89%</p>	<p>No Service Credits. Response times are detailed in Client Support Handbook.</p> <p>Support: 5 days a week, standard business hours</p> <p>Response Time: Direct Communication within 2 business hour.</p> <p>Updates: At a minimum 5 business day or mutually agreed upon frequency.</p>
Social Value - % of 'new hires' which will have trees planted, in line with Pega's 'one tree planted' pledge.	Social Value	(Number of requests made to include new hire in 'one tree planted' process / Total number of new hires in the reporting period, reported quarterly)	<p>Good Target: 100%</p> <p>Approaching Target: 90% - 99.9%</p> <p>Requires Improvement Target: 80% - 89.9%</p> <p>Inadequate Target: <80%</p>	No Service Credit. The Supplier shall continue with its social value commitments materially in line with the social value statement provided by the Supplier. The Buyer acknowledges that the type of social value commitments carried out by the Supplier change from time to time.

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2020

Part B: Performance Monitoring

3. Performance Monitoring and Performance Review

- 3.1 Not used
- 3.2 The Supplier provides performance monitoring at <https://status.pegasys.net/uptime>.
- 3.3 The Parties shall use the Operational Board (Schedule 15) to discuss Performance Monitoring on a monthly basis, where applicable / if any Service Levels have not been met. The Operational Board will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:
 - 3.3.1 be attended by the Supplier's Representative and the Buyer's Representative; and
 - 3.3.2 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.
- 3.4 The Buyer shall request such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

4. Satisfaction Surveys

- 4.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

Note: The parties agree that failure to meet KPI's alone does not constitute a material breach. The Social Value KPI is for reporting purposes only. Supplier shall use reasonable endeavours to comply with the Social Value KPI. However, Supplier may change its social value endeavours from time to time at its sole discretion. Supplier shall not be deemed to be in material breach should it not meet the social value KPI or change its social value endeavours.

Call-Off Schedule 14 (Service Levels)
Call-Off Ref:
Crown Copyright 2020

Call-Off Schedule 14 (Service Levels)
Call-Off Ref:
Crown Copyright 2020

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

Call-Off Ref:

Crown Copyright 2020

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 2020

- 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 Buyer 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 2020

Annex: Contract Boards

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

Operational Board

Monthly via online conferencing, or as mutually agreed.

Call-Off Schedule 20 (Call-Off Specification)
Call-Off Ref:
Crown Copyright 2020

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 for the duration of this Call off Contract.

1. The Authority requires subscription services for Pega Government Platform, and renewal of Pega Licences, with associated maintenance and support.
 - 1.1 Subscription services are required in the HRA's production environment for the entire lifecycle management of HRA clinical research studies, for the licensed number of annual Work Execution Cases, originating from or routed through the IRAS system, HARP or sub-systems, relating to the management of clinical research applications.
2. Work Execution Cases
 - 2.1 The subscription model for licences is based on the number of Work Execution Cases.
 - 2.2 A "Work Execution Case" means use of the Software for the creation, routing, updating, processing, tracking, completing and/or resolution of a single unit of work in a production environment, including directly updating other transaction systems.
 - 2.3 A single unit of work is an individual instance of the execution of a business process (whether processed as a stand-alone case or a related case within a more extensive business process) evidenced by an assigned unique numerical identifier.
 - 2.4 Case types can be found in Appendix A this Schedule 20.
3. Volumes
 - 3.1 The estimated number of Work Execution Cases anticipated in the first year of the contract is 38,000. This volume is anticipated to reduce over the contract term. No volumes are guaranteed.
 - 3.2 It is anticipated that any costs provided as part of a resultant procurement process will reflect potential reductions in volumes over the contract term.

Call-Off Schedule 20 (Call-Off Specification)

Call-Off Ref:

Crown Copyright 2020

4. Environments

4.1 The Authority requires the following environments as part of the service:

2 Standard Sandboxes	Each sandbox includes 50GB storage and supports a maximum of 15 developers and testers
1 Large Sandbox	Includes 100GB and supports a maximum of 45 developers and testers
1 Production Environment	Scaled to support the licenses and applications purchased

5. Storage

5.1 The Authority requires the following storage allowances as part of the service:

5.1.1 Production Data Storage - the storage of business data and rules data in the supplier database (1000 GB)

5.1.2 Production File Storage - the storage of files associated with features such as archive/purge, large attachment handling and file transfer services. (5000 GB)

6. Support Services

6.1 The Authority requires the following standard cloud support as part of the service offering:

- 24 x 7 x 365 monitoring and management of production services, including monitoring and management for database, environment, and network
- Security monitoring and management
- Service maintenance and updates, including patches and other updates for security, infrastructure, operating system, and supplier applications
- Disaster Recovery service
- Database backup and restore
- Threat and vulnerability testing

Call-Off Schedule 20 (Call-Off Specification)

Call-Off Ref:

Crown Copyright 2020

- Root cause analysis for Severity 1 events

The above services will be provided by the Supplier as per Client Support Handbook:

“**Client Support Handbook**” means the terms for Pegasystems’ provided support, upgrades, and updates located at: <https://docs.pega.com/supportpega-client-handbook/supportpega-client-handbook>, as may be periodically updated.

7. Additional Support

7.1 The Authority may require the following support in addition to the standard cloud support:

- Application Development problem management
- Issues encountered during standard use or testing
- Environmental issues, including performance and configuration problems with the product
- Installation, update, or migration problems
- Other software use or operation errors
- Assistance with isolating problems with non-supplier products, when appropriate.

Additional support to be agreed by way of a written amendment. _

8. Security and Vetting requirements

The Supplier must follow [The cloud security principles - NCSC.GOV.UK](https://www.ncsc.gov.uk/section-3)

[As per SaaS Terms and further service information as set out in Subscription Documentation below:](#)

“Subscription Documentation” means the specifications and operating guides associated with the Pega Cloud as published from time to time on Pegasystems’ web site at: <https://docs.pega.com/pega-cloud-services-subscription-documentation/pega-cloud-services-subscription-documentation>.

Appendix A

Call-Off Schedule 20 (Call-Off Specification)

Call-Off Ref:

Crown Copyright 2020

Case types and volumes

HRA Case Type	Definition
Initial submission (Project)	The original research proposal submitted for review to the regulators for approval.
Request for Further Information (RFI)	Used by the regulators to ask for more information, usually about the Initial Submission.
Amendment	A proposed change submitted by applicants to a study that has already improved; there are lots of different types of amendment which required different types of review.
Sponsor Representative Request (Account)	A request in New IRAS (see <i>Feedback</i> below) sent by an individual as a request to become a representative of an organisation. It must be approved by an existing member of the organisation.
Development Safety Update Report (DSUR)	DSURs are new, internationally-harmonised, safety documents (which became mandatory in European Union member states in September 2011) covering the safety summary of medicinal products during their development or clinical trial phase. The form in New IRAS can be submitted against multiple Projects.
Urgent Safety Measure (USM)	A measure that must be taken to protect clinical trial subjects due to an unexpected event that is likely to seriously affect the benefit-risk balance of the clinical trial. Form in New IRAS can be submitted against multiple Projects.
End of Trial (EOT)	Used to notify review bodies who approved the study and must be completed within 90 days of the study ending (global end date). In New IRAS this is a multi-part form also includes submission of the Clinical Summary of Results (CSR).
Clarification Request (INRFI)	A request for clarification following a response to an initial submission request for information or for further information about an End of Trial, Development Safety Update Report.
Feedback	A form available from a HRA IT system (New IRAS) which allows users to provide feedback on New IRAS. This is used by the User Feedback team to improve New IRAS.
Online Booking Function (OBF)	A supplier application which allows users to book REC meetings directly. The correct Research Ethics Committees (RECs) are selected by the user answering a series of questions. Much of the functionality of this workflow is managed within a specific HRA IT system as are all the meetings and bookings.
E-Submission of Amendment (EAA)	<p>A supplier platform for submitting all non-CTIMP amendments.</p> <p><i>A Clinical Trial of an Investigational Medicinal Product (CTIMP) is a clinical trial or study that is evaluating the safety or efficacy of a drug (Investigational Medicinal Product) or obtaining any other information about the drug e.g. how it is absorbed, distributed, metabolised or excreted.</i></p>

Requirement to incorporate possible volume changes for the case types - in particular the types cited below - over the duration of the contract in relation to the Customer's/Buyer's wider IT strategy and broader RSP programme. Volume changes, and reductions in particular, will be reflected in the Supplier's charges to the Customer/Buyer:

Call-Off Schedule 20 (Call-Off Specification)

Call-Off Ref:

Crown Copyright 2020

Case Type	Max annual nos.
Amendment	4,500
E-Submission of Amendment (EAA)	20,000

NOTE: should additional cases be required above 38,000 p.a. They can be purchased for the block pricing to be provided in the Order Form.

Call-Off Schedule 20 (Call-Off Specification)

Call-Off Ref:

Crown Copyright 2020

Call-Off Schedule 23 (Supplier-Furnished Terms)

Call-Off Ref:

Crown Copyright 2020

Call-Off Schedule 23 (Supplier-Furnished Terms)

Software as a Service (SaaS) Terms

1. Subscription Services.

- (a) If designated in an applicable Schedule, Pegasystems will provide Client with the Subscription Services in accordance with the Subscription Documentation to develop, test and/or deploy Client Applications within the Scope of Use. The Subscription Services include the Service Level Agreement. Client will be responsible for any Client managed or installed third-party products that are not included as part of the Subscription Services.
- (b) Client is responsible for the performance of any Client Application(s), for configuring Guardrail Compliant Client Application(s) in the Pega Cloud, and for complying with its obligations set forth in the Client Data Rights and Responsibilities, which is incorporated by reference.
- (c) Client will receive support, upgrades, and updates during the Term in accordance with the terms of the applicable Schedule and the Client Support Handbook.
- (d) Pegasystems will email to Client a URL to allow Client access to the Subscription Services. The Subscription Services will be accepted upon delivery. This acceptance is not dependent on any other contingencies or agreements.
- (e) Client acknowledges that in order for Pegasystems to provide the Subscription Services, Pegasystems may host, use, transmit and display Client Data, Client Applications and any third-party products, and may review Client's volume and type of usage of the Subscription Services. Pegasystems will not acquire any title or interest from Client in or to Client Data or third-party products.

2. Restrictions.

- (a) Client's use of the Subscription Services will comply with the terms of this Agreement, the Subscription Documentation, and Acceptable Use Policy. Client agrees not to sell, resell, rent, outsource, timeshare, lease or sublicense the Subscription Services to any third party or otherwise use it except as permitted under this Agreement and the applicable Schedule. Client will not use shared User IDs to avoid or reduce the counting of individuals that use the Subscription Services.
- (b) Client's use of the Subscription Services will be in object code and/or RuleSet form. Unless specifically authorized by law, Client may not reverse engineer, decompile, disassemble or otherwise attempt to determine source code or protocols from the Subscription Services.
- (c) Pegasystems owns all right, title and interest to the Subscription Services, Software, and Background Materials. The Software will contain Pegasystems' copyright notice and Client will reproduce such notice in any permitted copy made by Client.

3. Client Data and Security.

- (a) During the Term, Pegasystems will provide the Security Standards describing Pegasystems' information and physical security program (attached as Exhibit B to this Agreement).

4. Representations and Warranties.

- (a) Pegasystems warrants that:
 - i. the Subscription Services will operate substantially in accordance with the Subscription Documentation during the Term. If there is any failure of this warranty which can be replicated or verified, Pegasystems will, at its election, either promptly repair the Subscription Services to resolve such failure or terminate the Subscription Services and provide a refund for any pre-paid unused fees for the remaining portion

Call-Off Schedule 23 (Supplier-Furnished Terms)

Call-Off Ref:

Crown Copyright 2020

of the then current term of any Schedule(s) to which the breach relates. These remedies will be Client's exclusive remedy for any failures of the warranty in this Section 4(a)(i).

- ii. no disruptive or corrupting software that would damage, disable or compromise the security of a Client Application will be intentionally or knowingly introduced into the Subscription Services
- (b) To invoke the remedy described in Section 4(a)(i) Client must provide written notice to Pegasystems within the warranty period, expressly outlining the nature of the alleged failure or breach.
- (c) The foregoing warranties will be void to the extent that any failure of such warranties is caused by (i) anyone other than a Pegasystems employee modifying the Subscription Services (unless Pegasystems authorizes the specific change in writing), or (ii) non-Pegasystems' service, software, or hardware; or (iii) Client Applications that are non-Guardrail Compliant.
- (d) EXCEPT AS EXPRESSLY STATED IN THIS SECTION 4, PEGASYSTEMS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT.

5. Limitation of Liability

Notwithstanding any other provisions of the Agreement, Pegasystems' liability for any damages related to Client Data shall be limited to two times the amount of fees received by Pegasystems from Client in the prior twelve (12) months in connection with the Schedule(s) under which such damages arose, or to which such damages relate.

Call-Off Schedule 23 (Supplier-Furnished Terms)

Call-Off Ref:

Crown Copyright 2020

**EXHIBIT A
DEFINITIONS**

“Acceptable Use Policy” means the then current policy as published from time to time at <https://www.pega.com/acceptable-use>.

“Cloud Data Storage” means the storage of business data and rules data in the Pegasystems database that is available for the Production Environment only.

“Cloud File Storage” means the storage of files associated with features such as archive/purge, large attachment handling and file transfer services that is available across all Environments.

“Environment” means one of the following Pega Cloud deployments provided by Pegasystems:

- **“Standard Sandbox”** means a service that is intended to be used for development, functional/unit testing, UAT testing of Client Applications and training. A Standard Sandbox is scaled to support up to 15 developers/users with a storage limit of 50GB of Cloud Data Storage.
- **“Large Sandbox”** means a service that is intended to support development, functional/unit testing, UAT testing, pre-production, staging, and/or training of the Client Applications. A Large Sandbox is scaled to support up to 45 developers/users with a storage limit of 100GB of Cloud Data Storage.
- **“Production Environment”** means a service that is designed, built and scaled to accommodate Client Applications to process live and/or real-time data in connection with Client’s ongoing business operations and is deployed within a single geographic region. The Production Environment is scaled to support up to the licensed metrics defined in the Schedule.
- **“Production Mirror Sandbox”** means a replica of the scaled Production Environment that can be used for staging, scaled benchmark testing, and/or load performance testing or as defined in the applicable Schedule.

“Guardrail Compliant” means a Client Application with no severe warnings flagged by the Software and with a guardrail weighted score generated by the Software of ninety (90) or above as specified in the Subscription Documentation.

“Pega Cloud” means Pegasystems’ subscription-based offering of Pegasystems’ software capabilities for Client to build and run their Client Application(s) on Pegasystems’ operated environments.

“Service Level Agreement” means the Pega Cloud Production Environment availability as described at the following link: <https://docs.pega.com/pega-cloud-services-subscription-documentation/service-level-agreement-pega-cloud-services>.

“Subscription Documentation” means the specifications and operating guides associated with the Pega Cloud as published from time to time on Pegasystems’ web site at: <https://docs.pega.com/pega-cloud-services-subscription-documentation/pega-cloud-services-subscription-documentation>.

“Subscription Services” means the Pegasystems Software which is made available to Client for use on the Pega Cloud within the Scope of Use, including any enhancements, updates, upgrades, modifications, releases, Environments, data storage, or other services pursuant to an applicable Schedule.

Call-Off Schedule 23 (Supplier-Furnished Terms)

Call-Off Ref:

Crown Copyright 2020

EXHIBIT B SECURITY STANDARDS

1. **Security Practices & Review**

- 1.1. Pegasystems shall maintain an information and physical security program for the protection of Client personal information and confidential information in environments and on equipment controlled by Pegasystems (the “**Pegasystems Security Program**”).
- 1.2. As part of the Pegasystems Security Program, Pegasystems conducts periodic reviews of security practices against various leading industry standards, such as NIST, ISO 27001 and SSAE18 SOC2. Pegasystems regularly re-evaluates and updates the Pegasystems Security Program as the industry evolves, new technologies emerge, or new threats are identified. Upon request, Pega will maintain and make available on at least an annual basis, a reasonable information security questionnaire completed with answers concerning Pegasystems Security Program specific to the services provided under the applicable Schedule.
- 1.3. The Pegasystems Security Program consists of the following:

a. **Physical Access**

Pegasystems maintains physical security standards designed to prohibit unauthorized physical access to Pegasystems facilities and equipment. This is accomplished by the following practices:

- physical access to locations is limited to Pegasystems employees, subcontractors and authorized visitors;
- Pegasystems employees, subcontractors and authorized visitors are issued identification cards that must be worn while on premises;
- monitoring access to Pegasystems facilities, including restricted areas and equipment within Pegasystems facilities;
- all access to the data centers where customer personal data is hosted is logged, monitored, and tracked; and
- data centers are secured with alarm systems and video cameras.

b. **Access Control and Administration**

Pegasystems maintains the following standards for access control and administration in environments and on equipment controlled by Pegasystems or Pegasystems contractors.

- administrator accounts are only be used for the purpose of performing administrative activities;
- each account with administrative privileges must be traceable to a uniquely-identifiable individual;
- all access to computers and servers must be authenticated and within the scope of an employee's job function;
- initial passwords must be changed by the user on first use;
- the display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them;

Call-Off Schedule 23 (Supplier-Furnished Terms)

Call-Off Ref:

Crown Copyright 2020

- passwords must be uniquely identifiable to an individual;
- passwords must be encrypted when transmitted or stored;
- password complexity should never be less than 3 out of 4-character classes and must have character class choices such as upper-case letters, lower case letters, numeric digits, or special characters;
- passwords must not contain 3 or more identical consecutive characters;
- password length must be configured to be at least 12 characters;
- passwords shall expire between 90 and 180 days depending on its length; 12 characters – 90 days, 16 characters – 135 days, 20+ characters – 180 days;
- automatic time-out of access to computers and servers if left idle with the requirement for password authentication for re-access; and
- per Pega policy, accounts must be set to lockout after six erroneous failed login attempts.

c. Virus Scanning and Logging

- Computers and servers have commercially reasonable up-to-date versions of system security software which may include host firewall, anti-virus protection and up-to-date patches and virus definitions. Such software is configured to scan for and promptly remove or fix identified findings.
- Pegasystems maintains logs of various components of the infrastructure and an intrusion detection system to monitor, detect, and report misuse patterns, suspicious activities, unauthorized users, and other actual and threatened security risks.

d. Encryption

- Pega encrypts all data in transit over public networks.
- Data originating from or residing within Pega networks is encrypted at rest.

2. Pegasystems Personnel

- 2.1. Employees and contractors are required by policy to be trained on Pegasystems' privacy and security policies and made aware of their responsibilities regarding privacy and security practices.
- 2.2. Pegasystems employees and contractors are contractually bound to maintain the confidence of Client personal information or confidential information and comply with applicable Pegasystems policies, standards or requirements in relation to the processing of Client personal information. Failure to comply with those policies, standards or requirements will be subject to investigation which may result in disciplinary action up to and including termination of employment or engagement by Pegasystems and legal action as appropriate.

3. Security Breach Notification and Security Incident Management

- 3.1. Pegasystems will notify Client within twenty-four (24) hours of becoming aware of a Security Incident. A "**Security Incident**" means the unauthorized access to or use of Client information on environments or equipment controlled by Pegasystems affecting the confidentiality, availability and integrity of such Client confidential information. Pegasystems will provide Client with updates on the status of the Security Incident until the matter has

Call-Off Schedule 23 (Supplier-Furnished Terms)

Call-Off Ref:

Crown Copyright 2020

been remediated. The reports will include, without limitation, a description of the Security Incident, actions taken and remediation plans.

- Notice of a Security Incident shall be sent via email to the security contacts that Client designates in its Pega Support Portal (found here: <https://msp.pegacom>).
- Similarly, if Client becomes aware of a Security Incident that affects the Services, Client shall, without undue delay, notify Pegasystems of such and inform Pegasystems of the scope of the Security Incident. Such notice from Client to Pegasystems should be provided to: SecurityBreachNotice@pegacom and/or 1-617-866-6800.

3.2 Proportionate to acts or omissions of Pegasystems resulting in a Security Incident, and subject to terms and limitations set forth in the Agreement, Pegasystems agrees to pay reasonable costs for: (i) required notice to individuals affected by the Security Incident; and (ii) credit monitoring service for twelve months for affected data subjects, except to the extent applicable law specifies a longer period for applicable credit monitoring services, in which case such longer period shall then apply.

3.3 Pegasystems will, at the request and cost of the Client:

- Provide reasonable assistance to the Client in notifying a Security Incident to the supervisory authority competent under the privacy laws applicable to the Client; and
- Provide reasonable assistance to the Client in communicating a Security Incident to data subjects in cases where the Security Incident is likely to result in a high risk to the rights and freedoms of individuals.

APPENDIX 1.



Crown
Commercial
Service

Core Terms

Notes:

Updated Core Terms with HRA

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, unused and of recent origin.

3.2.2 All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.

3.2.3 **Not used.**

3.2.4 **Not used.**

3.2.5 **The Supplier warrants that it has the right to grant a license for use of the Goods to the Buyer.**

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 **Not used.**

- 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 **Not used.**
- 3.2.12 **Not used.**

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 **Not used.**
- 4.10 **Not used.**
- 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 GDPR,
- The Supplier is not required to provide any information in relation to Open Book Data.**
- 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

Core Terms

(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 licence to use 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 **during the term of this Call-Off. Supplier owns all right, title and interest to the Supplier Software and permits Buyer to use during the term of this Call-Off.**

"Software" means the Supplier software listed in this Call-Off, including any enhancements, updates, upgrades, modifications, or other releases provided to Buyer.

- 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.
- 10.2.1a The Call-Off shall survive any termination by CCS of the Framework under clause 10.2.1 and the Call-Off shall continue and does not give Buyer right to terminate because of any termination by CCS under 10.2.1.
- 10.2.2 The Buyer has the right to terminate this Call-Off Contract without reason by giving the Supplier not less than 90 days' written notice in advance, provided that, if Buyer does serve notice under this provision the Buyer remains liable to pay any outstanding fees that would have been payable during the Call Off Initial Period. If the Call Off Contract is extended, same shall apply for the extended period (so for the 12-month extended period, fees for the 12 months would be due).

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.
- 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 **material** 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 material 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. **The Buyer acknowledges that because the software is configurable by the Buyer, it is the Buyer that chooses how the software is configured and any liability arising from that and any other Buyer related actions are attributable to Buyer and not the Supplier, whether the configuration is done by Supplier on the Buyers direction, a third party working for Buyer, or Buyers own staff.**

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) Not used
- (b) Not used
- (c) Not used
- (d) any of the events in 73 (1) (a) or (c) of the Regulations happen-

10.5 When the supplier can end the contract

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 10.2.2, 10.4.1, 10.4.2, 10.4.3, 10.5 or 20.2 or a Contract expires all of the following apply:

- (a) **Subject to 10.2.2**, 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

Core Terms

respect of Deliverables not provided by the Supplier as at the End Date , notwithstanding annual subscription charges, paid in advance, will not be reimbursed if the termination is due to a non-fault based event, under 10.4.3.

- (d) The Supplier must promptly delete or return the Buyer's 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, co-operate fully in the handover and re-procurement (including to a Replacement Supplier), **subject to Call Off Schedule 10 (Exit)**.

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, **subject to the limits of liabilities agreed under this Call-Off**.

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

Not used.

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 125% of the Estimated Yearly Charges.

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 125% 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, which for the purposes of this Call Off Contract is deemed to be £1,000,000.

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.

12.4 **Compliance with Export Controls Laws.** The export and re-export of the Pegasystems Software and Technology is subject to the export control and sanctions laws, regulations, and orders of the United States, including but not limited to the Export Administration Regulations ("EAR"), International Traffic in Arms Regulations ("ITAR"), and regulations and orders administered by the Treasury Department's Office of Foreign Assets Control ("OFAC") (collectively, "Export Control Laws"). Buyer agrees that it will not export, reexport, transfer, or allow access to the Pegasystems Software and Technology: (a) to or by parties on lists of sanctioned or restricted parties maintained by the U.S. government, including but not limited to OFAC, the U.S. Department of Commerce, or the U.S. Department of State; (b) to or by parties in or relating to certain countries or territories that are the target of U.S. sanctions (currently, Cuba, Iran, Syria, North Korea, and the Crimea region of Ukraine); or (c) otherwise in violation of Export Control Laws. The export and re-export of the Pegasystems Software and Technology may also be subject to export and import controls under the laws and regulations of other countries. Buyer agrees, at all times, to comply fully with the Export Control Laws and the local export and import controls of other countries.

13. Insurance

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).

Core Terms

- 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 if Buyer is not able to retrieve the same itself after having raised a ticket with the Supplier;
 - (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

Core Terms

- (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

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

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

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

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

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

Core Terms

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 or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and
- (b) 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

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