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

Order Form

CALL-OFF REFERENCE: C397243

THE BUYER: The Secretary of State for Health and Social Care as part of the Crown through the UK Health Security Agency

(Also referred to as "UKHSA")

BUYER ADDRESS 10 South Colonnade,
Canary Wharf,
London,
E14 4PU.

THE SUPPLIER: AKHTER COMPUTERS LIMITED

SUPPLIER ADDRESS: 1-3 Marshgate Business Centre,
Harlow Business Park,
Harlow, CM19 5QP

REGISTRATION NUMBER: [redacted]

DUNS NUMBER: [redacted]

SID4GOV ID: **N/A**

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 30th October 2025. It's issued under the Framework Contract with the reference number RM6098 for the provision of Technology Products & Associated Service 2.

CALL-OFF LOT(S):

Lot 1: Hardware and Software and Associated Services

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) RM6098
3. Framework Special Terms
4. The following Schedules in equal order of precedence:

    - Joint Schedules for RM6098
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)

- Joint Schedule 5(corporate social responsibility)
- Optional Terms for (Bronze Contracts)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

- Call-Off Schedules for RM6098

  Call-Off Schedule 1 (Transparency Reports)

  Call-off schedule 4 (Call-Off Tender)

  Call-off schedule 5 (Pricing Details)

  Call-Off Schedule 9 (Security): Include only Part A, paragraphs 2.1, 3.1, 3.2 (excluding 3.2.4), 3.3, and 3.4. Exclude Paragraphs 4 and 5.

  Call off schedule 15 (Call- off contract management):
  Exclude Paragraph 4

  Call off schedule 20 (Specification)

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

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 save for the Cloudian end user licence terms at Special Term 1.

CALL-OFF SPECIAL TERMS

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

Special Terms 1: Cloudian Third-party terms

The following Cloudian documents are incorporated into this Agreement as set out in Appendix 1 solely for the purposes described below:

- Cloudian End User License Agreement (EULA): Incorporated solely to define the licensing conditions applicable to the Cloudian products and services.
- Cloudian technical Support and product life cycle : Incorporated to ensure the agreed service levels for technical support apply to the Buyer.
- Goods Terms: Incorporated to ensure the applicable warranty obligations for the Goods are enforceable by the Buyer.

The Buyer shall comply with these Cloudian terms only to the extent necessary for lawful use of the Cloudian products and services and to benefit from the support and warranty obligations. In the event of any conflict between this Agreement and the Cloudian terms, this Agreement shall prevail, except where specific Cloudian licensing provisions, support obligations, or warranty terms are mandatory for lawful use or enforceability of the Goods and services.

Commencement date:	The date this Agreement is signed by both Parties.
Effective date:	The date on which the Goods are delivered and formally accepted by the Authority
Expiry Date:	Five (5) years from the effective Date

CALL-OFF DELIVERABLES

[redacted]

TOTAL COST OF OWNERSHIP FOR 60 MONTHS EX VAT	£387,156.65

LOCATION FOR DELIVERY

The Authority requires delivery and installation and commissioning of all Cloudian hardware and software and support to the listed sites within UK:

1. Chilton
UK Health Security Agency
Chilton Didcot, Oxon OX11 0RQ UK

Contacts:

[redacted]

2. Porton Down
UK Health Security Agency
Porton Down, Manor Farm Road, Porton Down, Nr Salisbury, Wiltshire, SP4 0JG

Contacts:

[redacted]

3. Colindale
UK Health Security Agency
61 Colindale Ave, London NW9 5EQ

Contacts:

[redacted]

DATES FOR DELIVERY AND INSTALLATION

1. The supplier shall deliver the goods to the Authority's nominated delivery location on a date to be agreed in writing between the parties ("Delivery Date").

2. The supplier shall notify the Authority of the proposed delivery date within Ten (10) working days of the commencement date.

3. Installation and commissioning of the hardware and software shall commence promptly after delivery. The supplier shall confirm the installation and commissioning schedule when providing the delivery date.

WARRANTY PERIOD

For the purposes of Clause 3.1.2 of the Core Terms, the warranty period for hardware shall be five (5) years from the date of delivery, aligned with the duration of the support services. This warranty covers defects in materials and workmanship under normal use and includes repair or replacement obligations as defined in the support agreement.

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 £387,156.65 Ex Vat, Estimated Charges in the first 12 months of the Contract.

CALL-OFF CHARGES

The charges for this Call-Off Contract are set out in Call-Off Schedule 5 (Charges).

Payment terms

In accordance with Clause 3.2 of the Core Terms, the Supplier may only issue an invoice once the Goods have been delivered. As per Clause 4.4, the Buyer shall pay the Supplier all of the Charges within thirty (30) calendar days of receipt of a valid and undisputed invoice, in cleared funds, using the payment method and details stated in the Order form

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

BACS

BUYER'S INVOICE ADDRESS:

Accounts Payable;

UK Health Security Agency,

Manor Farm Road,

Porton Down,

Salisbury,

SP4 0JG

[redacted]

BUYER'S AUTHORISED REPRESENTATIVE

Name: Gareth Munday

Title: [redacted]

Email: [redacted]

Name: Stacey Ahern

Title: Commercial Lead

Email: [redacted]

BUYER'S ENVIRONMENTAL POLICY

Not Applicable

BUYER'S SECURITY POLICY

Appended at Call-Off Schedule 9 (Security): only Paragraphs 2.1, 3.1, 3.2 (excluding 3.2.4), 3.3, and 3.4 shall apply. Paragraphs 4 and 5 are excluded.

Part A: Short Form Security Requirements shall apply to this Call-Off Contract. **Part B** is not used.

SUPPLIER'S AUTHORISED REPRESENTATIVE

Name: Lisa Smyth

Email: [redacted]

SUPPLIER'S CONTRACT MANAGER

Name: Lisa Smyth

Email: [redacted]

PROGRESS REPORT FREQUENCY

As and when required by the customer

PROGRESS MEETING FREQUENCY

As and when required by the customer

KEY STAFF

Not Applicable

KEY SUBCONTRACTOR(S)

Not applicable

COMMERCIALLY SENSITIVE INFORMATION

Call off schedule 5 (pricing details)

SERVICE CREDITS

Not applicable

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

The Supplier's social value proposal, as evaluated during the tender process, forms an integral part of this contract. Over the 60-month support period, the Supplier shall deliver on its commitments to environmental sustainability, including energy-efficient system setup, reduced power and cooling requirements, responsible handling of replaced components, and end-of-life recycling to minimise e-waste and avoid landfill. These obligations contribute directly to the Policy Outcome and Award Criteria and will be monitored throughout the contract term.

For and on behalf of the Supplier:	**For and on behalf of the Buyer:**
[redacted]	Signed by [redacted]
Job Title/Role: Contracts Manager	Job Title/Role: Commercial Manager
Date Signed: 25/11/2025	Date Signed: 26/11/2025

Joint Schedule 1 (Definitions)

1.1 In each Contract, unless the context otherwise requires, capitalized expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalized expression appears.

1.2 If a capitalized expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.

1.3 In each Contract, unless the context otherwise requires:

1.3.1 the singular includes the plural and vice versa;

1.3.2 reference to a gender includes the other gender and the neuter;

1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Central Government Body;

1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.3.5 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";

1.3.6 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;

1.3.7 references to "**representations**" shall be construed as references to present facts, to "**warranties**" as references to present and future facts and to

"**undertakings"** as references to obligations under the Contract;

1.3.8 references to **"Clauses"** and **"Schedules"** are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;

1.3.9 references to **"Paragraphs"** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;

1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;

1.3.11 the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract;

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

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

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

(b) any EU institution or EU authority or other such EU body shall be read on and after Exit Day as a reference to the UK institution, authority or body to which its functions were transferred; and

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

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

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

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

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);

a) 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;

b) verify the Open Book Data;

c) verify the Supplier's and each Subcontractor's compliance with the Contract and applicable Law;

d) 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;

e) 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;

f) 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;

g) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract;

h) 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;

i) enable the National Audit Office to carry out an examination pursuant to Section 6(1) o

	the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant Authority has used its resources; or k) verify the accuracy and completeness of any Management Information delivered or required by the Framework Contract;
Auditor"	a) the Relevant Authority's internal and external auditors; b) the Relevant Authority's statutory or regulatory auditors; c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; d) HM Treasury or the Cabinet Office; e) any party formally appointed by the Relevant Authority to carry out audit or similar
	review functions; and f) successors or assigns of any of the above;

Call-Off Tender"	the tender submitted by the Supplier in response to the Buyer's Statemen of Requirements following a Further Competition Procedure and set out at Call-Off Schedule 4 (Call-Off Tender);
CCS"	the Minister for the Cabinet Office as represented by Crown Commerci Service, which is an executive agency and operates as a trading fund the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP;
CCS Authorised representative"	the representative appointed by CCS from time to time in relation to the Framework Contract initially identified in the Framework Award Form;
Central government body"	a body listed in one of the following sub-categories of the Centra Government classification of the Public Sector Classification Guide, a published and amended from time to time by the Office for Nationa Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;
Change in Law"	any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date;
Change of control"	a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;
Charges"	the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Call-Off Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Call-

	Off Contract less any Deductions;
Claim"	any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract;
Commercially sensitive information"	the Confidential Information listed in the Framework Award Form or Orde 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 th business, affairs, developments, trade secrets, Know-How, personnel an 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;
Conflict of interest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS;
Contract"	either the Framework Contract or the Call-Off Contract, as the context requires;
Contract Period"	the term of either a Framework Contract or Call-Off Contract on and from the earlier of the: a) applicable Start Date; or b) the Effective Date up to and including the applicable End Date;
Contract Value"	the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier;
Contract Year"	a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof;
Control"	control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "**Controlled**" shall be construed accordingly;
Controller"	has the meaning given to it in the UK GDPR;
Core Terms"	CCS' terms and conditions for common goods and services which govern how Suppliers must interact with CCS and Buyers under Framework Contracts and Call-Off Contracts;

Costs"	the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables: a) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Workday, 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) workplace accommodation; viii) workplace 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;

	b) costs incurred in respect of Supplier Assets which would be treated as capita 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 not held by the Supplier) any cost actually incurred by the Supplier in respect o those Supplier Assets; c) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables; and d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables; but excluding: e) Overhead; f) financing or similar costs; g) maintenance and support costs to the extent that these relate to maintenanc and/or support Deliverables provided beyond the Call-Off Contract Perio whether in relation to Supplier Assets or otherwise; h) taxation; i) fines and penalties; j) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and k) non-cash items (including depreciation, amortization, impairments and movements in provisions).
CRTPA"	the Contract Rights of Third Parties Act 1999;

"Cyber essentials equivalent"	ISO27001 certification where: a) the Cyber Essentials requirements, at either basic or Plus levels as appropriate, have been included in the scope, and verified as such; and b) the certification body carrying out this verification is approved to issue a Cyber Essentials certificate by one of the accreditation bodies This would be regarded as holding an equivalent standard to Cyber Essentials.
Data Protection impact assessment"	an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
Data Protection legislation"	(I) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy;
Data Protection liability Cap"	the amount specified in the Framework Award Form;

Data Protection officer"	has the meaning given to it in the UK GDPR;
Data Subject"	has the meaning given to it in the UK GDPR;
Data Subject access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
Deductions"	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under a Call-Off Contract;

Default"	any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority;
Default management charge"	has the meaning given to it in Paragraph 8.1.1 of Framework Schedule 5 (Management Charges and Information);
Delay Payments"	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
Deliverables"	Goods and/or Services that may be ordered under the Contract including the Documentation;
Delivery"	delivery of the relevant Deliverable or Milestone in accordance with the terms of a Call-Off Contract as confirmed and accepted by the Buyer by either (a confirmation in writing to the Supplier; or (b) where Call-Off Schedule 13 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. "**Deliver**" and "**Delivered**" shall be construed accordingly;
Disclosing Party"	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);
Dispute"	any claim, dispute or difference (whether contractual or non-contractual) arisin out of or in connection with the Contract or in connection with the negotiatio existence, legal validity, enforceability or termination of the Contract, whether th alleged liability shall arise under English law or under the law of some other countr and regardless of whether a particular cause of action may successfully be brough in the English courts;

Dispute resolution procedure"	the dispute resolution procedure set out in Clause 34 (Resolving disputes);
Documentation"	descriptions of the Services and Service Levels, technical specifications, use 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:

	l) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deplo run, maintain, upgrade and test the individual systems that provide the Deliverables m) is required by the Supplier in order to provide the Deliverables; and/or n) has been or shall be generated for the purpose of providing the Deliverables;
DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of Ta schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within se time limits as contained in Part 7 of the Finance Act 2004 and in secondar 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 structure electronic format which allows for its automatic and electronic processing and which complies with (a) the European standard and (b) any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870;
Employment regulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC;
End Date"	the earlier of: a) the Expiry Date (as extended by any Extension Period exercised by the Relevant Authority under Clause 10.1.2); or b) 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 an phase out the use of ozone depleting substances and minimise the release o greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the
	Buyer;
Equality and human Rights commission"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
Estimated Year 1 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;
"**Exempt Buyer**"	a public sector purchaser that is: a) eligible to use the Framework Contract; and b) is entering into an Exempt Call-off Contract that is not subject to (as applicable) any of: i) the Regulations; ii) the Concession Contracts Regulations 2016 (SI 2016/273); iii) the Utilities Contracts Regulations 2016 (SI 2016/274); iv) the Defense and Security Public Contracts Regulations 2011 (SI 2011/1848); v) the Remedies Directive (2007/66/EC); vi) Directive 2014/23/EU of the European Parliament and Council; vii) Directive 2014/24/EU of the European Parliament and Council; viii) Directive 2014/25/EU of the European Parliament and

	Council; or ix) Directive 2009/81/EC of the European Parliament and Council;
"**Exempt Call-off Contract**"	the contract between the Exempt Buyer and the Supplier for Deliverables which consists of the terms set out and referred to in the Order Form incorporating and, where necessary, amending, refining or adding to the terms of the Framework Contract;
"**Exempt Procurement Amendments**"	any amendments, refinements or additions to any of the terms of the Framework Contract made through the Exempt Call-off Contract to reflect the specific needs of an Exempt Buyer to the extent permitted by and in accordance with any legal requirements applicable to that Exempt Buyer;

Existing IPR"	any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise);
Exit Day"	shall have the meaning in the European Union (Withdrawal) Act 2018;
Expiry Date"	the Framework Expiry Date or the Call-Off Expiry Date (as the context dictates);
Extension Period"	the Framework Optional Extension Period or the Call-Off Optional Extension Period as the context dictates;

"Financial Reports"	a report by the Supplier to the Buyer that: a) provides a true and fair reflection of the Costs and Supplier Profit Margin forecast by the Supplier; b) provides a true and fair reflection of the costs and expenses to be incurred by Key Subcontractors (as requested by the Buyer); c) is in the same software package (Microsoft Excel or Microsoft Word), layout and format as the blank templates which have been issued by the Buyer to the Supplier on or before the Start Date for the purposes of the Contract; and is certified by the Supplier's Chief Financial Officer or Director of Finance;
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 practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
Force Majeure vent"	any event outside the reasonable control of either Party affecting it performance of its obligations under the Contract arising from acts, event omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any willful act, neglect or failure to take reasonable preventative action by that Party, including: a) riots, civil commotion, war or armed conflict; b) acts of terrorism; c) acts of government, local government or regulatory bodies; d) fire, flood, storm or earthquake or other natural disaster, but excluding any industrial dispute relating to the Supplier, the Supplier Staff or any other failure in the Supplier or the Subcontractor's supply chain;

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 i accordance with Regulation 33 by the Framework Award Form for the provisio of the Deliverables to Buyers by the Supplier pursuant to the notice published on the Find a Tender Service;
Framework Contract period"	the period from the Framework Start Date until the End Date of the Framework Contract;
Framework Expiry ate"	the scheduled date of the end of the Framework Contract as stated in the Framework Award Form;
Framework incorporated Terms"	the contractual terms applicable to the Framework Contract specified in the Framework Award Form;
Framework Optional extension Period"	such period or periods beyond which the Framework Contract Period may be extended as specified in the Framework Award Form;
Framework Price(s)"	the price(s) applicable to the provision of the Deliverables set out in Framework Schedule 3 (Framework Prices);
Framework Special terms"	any additional terms and conditions specified in the Framework Award Form incorporated into the Framework Contract;

Framework Start ate"	the date of start of the Framework Contract as stated in the Framework Award Form;
Framework Tender response"	the tender submitted by the Supplier to CCS and annexed to or referred to in Framework Schedule 2 (Framework Tender);
Further Competition procedure"	the further competition procedure described in Framework Schedule 7 (Call-Off Award Procedure);
UK GDPR"	the retained EU law version of the General Data Protection Regulation
	(Regulation (EU) 2016/679);
General Anti-Abuse rule"	a) the legislation in Part 5 of the Finance Act 2013 and; and b) any future legislation introduced into parliament to counteract Tax advantages arising from abusive arrangements to avoid National Insurance contributions;
General Change in law"	a Change in Law where the change is of a general legislative nature (including Tax or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"Gold Contract"	a Call-Off Contract categorized as a gold contract using the Cabinet Office Contract Tiering Tool;
Goods"	goods made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form;
Good Industry practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence 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 Irelan Assembly and Executive Committee, the Scottish Government and th National Assembly for Wales), including government ministers an government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
Government Data"	the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which: i) are supplied to the Supplier by or on behalf of the Authority; or ii) the Supplier is required to generate, process, store or transmit pursuant to a Contract;
Guarantor"	the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract;
Halifax Abuse principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
"HM Government"	Her Majesty's Government;
HMRC"	Her Majesty's Revenue and Customs;
ICT Policy"	the Buyer's policy in respect of information and communications technolog referred to in the Order Form, which is in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;

Impact Assessment"	an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including: a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract; b) details of the cost of implementing the proposed Variation; c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Framework Prices/Charges (as applicable), any alteration in the resources and/o expenditure required by either Party and any alteration to the working
	practices of either Party; d) a timetable for the implementation, together with any proposals for the testing of the Variation; and e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;

Implementation plan"	the plan for provision of the Deliverables set out in Call-Off Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;
Indemnifier"	a Party from whom an indemnity is sought under this Contract;
Independent control"	where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and "Independent Controller" shall be construed accordingly;
Indexation"	the adjustment of an amount or sum in accordance with Framework Schedule 3 (Framework Prices) and the relevant Order Form;
Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
Information commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
Initial Period"	the initial term of a Contract specified in the Framework Award Form or the Order Form, as the context requires;

Insolvency Event"	with respect to any person, means: (a) that person suspends, or threatens to suspend, payment of its debts, o is unable to pay its debts as they fall due or admits inability to pay its debts or: (i) (being a company or an LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or (ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986; (b) that person commences negotiations with one or more of its creditors (using a voluntar arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, o makes a proposal for or enters into any compromise or arrangement with one or more of its creditor or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 the Insolvenc Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solven reconstruction of that person; (c) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person; (d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on o sued against, the whole or any part of that person's assets and such attachment or process is not discharged within 14 days;

	(e) that person suspends or ceases, or threatens to suspend or cease carrying on all or a substantial part of its business; (f) where that person is a company, an LLP or a partnership: (i) a petition is presented (which is not dismissed within 14 days of its service), a notice is given, a resolution is passed, or an order is made, for o in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person; (ii) an application is made to court, or an order is made, for the appointmen of an administrator, or if a notice of intention to appoint an administrator filed at Court or given or if an administrator is appointed, over that person; (iii) (being a company or an LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or ha appointed an administrative receiver; or (iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or (g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above;
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- Of Contract;

Intellectual Property rights" or "IPR"	a) copyright, rights related to or affording protection similar to copyright rights in databases, patents and rights in inventions, semi-conductor topography rights, trademarks, 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; b) applications for registration, and the right to apply for registration, for an of the rights listed at (a) that are capable of being registered in any countr or jurisdiction; and c) all other rights having equivalent or similar effect in any country o jurisdiction;
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 defense 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 compan pay the same income tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies;
"ISO"	International Organization for Standardization;
Joint Controller agreement"	the agreement (if any) entered into between the Relevant Authority and the Supplier substantially in the form set out in Annex 2 of Joint Schedule 11 (*Processing Data*);
Joint Controllers"	where two or more Controllers jointly determine the purposes and means of Processing;
Key Staff"	the individuals (if any) identified as such in the Order Form;
Key Sub-Contract"	each Sub-Contract with a Key Subcontractor;
Key Subcontractor"	any Subcontractor: a) which is relied upon to deliver any work package within the Deliverable in their entirety; and/or b) which, in the opinion of CCS or the Buyer performs (or would perform appointed) a critical role in the provision of all or any part of th Deliverables; and/or c) with a Sub-Contract with a contract value which at the time of appointmen exceeds (or would exceed if appointed) 10% of the aggregate Charge forecast to be payable under the Call-Off Contract, and the Supplier shall list all such Key Subcontractors in section 19 of the Framework Award Form and in the Key Subcontractor Section in Order Form;

Know-How"	all ideas, concepts, schemes, information, knowledge, techniques methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date;
Law"	any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, byelaw, enforceable right within the meaning o Section 2 of the European Communities Act 1972, regulation, orde regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply;
Losses"	all losses, liabilities, damages, costs, expenses (including legal fees) disbursements, costs of investigation, litigation, settlement, judgment interest and penalties whether arising in contract, tort (including negligence) breach of statutory duty, misrepresentation or otherwise and "**Loss**" shall be interpreted accordingly;
Lots"	the number of lots specified in Framework Schedule 1 (Specification), if applicable;

Management charge"	the sum specified in the Framework Award Form payable by the Supplier to CCS in accordance with Framework Schedule 5 (Management Charges and Information);
Management information" or "MI"	the management information specified in Framework Schedule 5 (Management Charges and Information);
MI Default"	means when two (2) MI Reports are not provided in any rolling six (6) month period
MI Failure"	means when an MI report: a) contains any material errors or material omissions or a missing mandatory field; or b) is submitted using an incorrect MI reporting Template; or c) is not submitted by the reporting date (including where a declaration of no business should have been filed);
MI Report"	means a report containing Management Information submitted to the Authority in accordance with Framework Schedule 5 (Management Charges and Information);
MIReporting template"	means the form of report set out in the Annex to Framework Schedule 5 (Management Charges and Information) setting out the information the Supplier is required to supply to the Authority;
Milestone"	an event or task described in the Implementation Plan;
Milestone Date"	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved;
Month"	a calendar month and "**Monthly**" shall be interpreted accordingly;
National Insurance"	contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions)

	Regulations 2001 (SI 2001/1004);
New IPR"	a) IPR in items created by the Supplier (or by a third party on behalf of th Supplier) specifically for the purposes of a Contract and updates an amendments of these items including (but not limited to) databas schema; and/or b) IPR in or arising as a result of the performance of the Supplier's obligation under a Contract and all updates and amendments to the same; but shall not include the Supplier's Existing IPR;
Occasion of Tax on– Compliance"	where: a) any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of: 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

	that have an effect equivalent or similar to the General Anti- Abuse Rule or the Halifax Abuse Principle; ii) the failure of an avoidance scheme which the Supplier was involved in and which was, or should have been, notified to a Relevant Ta Authority under the DOTAS or any equivalent or similar regime in an jurisdiction; and/or b) any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a crimina 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;

Open Book Data "	complete and accurate financial and non-financial information which i 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-Of Contrac including details and all assumptions relating to: a) the Supplier's Costs broken down against each Good and/or Servic and/or Deliverable, including actual capital expenditure (including capit replacement costs) and the unit cost and total actual costs of Deliverables; b) operating expenditure relating to the provision of the Deliverable including an analysis showing: i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables; ii) staff costs broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each grade; iii) a list of Costs underpinning those rates for each grade, being the agreed rate less the Supplier Profit Margin; and iv) Reimbursable Expenses, if allowed under the Order Form; c) Overheads; d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables; e) the Supplier Profit achieved over the Framework Contract Period and on an annual basis; f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods

	applied generally by the Supplier; g) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of mone attributed to each risk and/or contingency; and h) the actual Costs profile for each Service Period;

Order"	means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;
Order Form"	a completed Order Form Template (or equivalent information issued by the Buyer) used to create a Call-Off Contract;
Order Form template"	the template in Framework Schedule 6 (Order Form Template and Call-Off Schedules);

Other Contracting authority"	any actual or potential Buyer under the Framework Contract;
Overhead"	those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs";
Parliament"	takes its natural meaning as interpreted by Law;
Party"	in the context of the Framework Contract, CCS or the Supplier, and in the in the context of a Call-Off Contract the Buyer or the Supplier. "**Parties**" shall mean both of them where the context permits;
Performance indicators" or "PIs"	the performance measurements and targets in respect of the Supplier's performance of the Framework Contract set out in Framework Schedule 4 (Framework Management);
Personal Data"	has the meaning given to it in the UK GDPR;
Personal Data reach"	has the meaning given to it in the UK GDPR;
Personnel"	all directors, officers, employees, agents, consultants and suppliers of a Party and/or of any Subcontractor and/or Sub processor engaged in the performance of its obligations under a Contract;
Prescribed Person"	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle- list-of-prescribed-people-and-bodies--2/whistleblowing-list-of- prescribed-people-and-bodies;

Processing"	has the meaning given to it in the UK GDPR;
Processor"	has the meaning given to it in the UK GDPR;
Progress Meeting"	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;
Progress Meeting frequency"	the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form;
Progress Report"	a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates;

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"	a) to directly or indirectly offer, promise or give any person working for o engaged by a Buyer or any other public body a financial or other advantage to: i) induce that person to perform improperly a relevant function or activity or ii) reward that person for improper performance of a relevant function of activity; b) to directly or indirectly request, agree to receive or accept any financial o other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with each Contract; or c) committing any offence: i) under the Bribery Act 2010 (or any legislation repealed or revoked b 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 d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;

Protective measures”	appropriate technical and organizational measures which may include pseudonymizing and encrypting Personal Data, ensuring confidentialit integrity, availability and resilience of systems and services, ensuring tha availability of and access to Personal Data can be restored in a timely manne after an incident, and regularly assessing and evaluating the effectiveness o the such measures adopted by it including those outlined in Framewor Schedule 9 (Cyber Essentials Scheme), if applicable, in the case of the Framework Contract or Call-Off Schedule 9 (Security), if applicable, in the case of a Call-Off Contract.
“Rating Agency”	as defined in the Framework Award Form or the Order Form, as the context requires;
Recall”	a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance;
Recipient Party"	the Party which receives or obtains directly or indirectly Confidential Information;
Rectification Plan"	the Supplier’s plan (or revised plan) to rectify its breach using the template in Joint Schedule 10 (Rectification Plan) which shall include:

	a) full details of the Default that has occurred, including a root cause analysis; b) the actual or anticipated effect of the Default; and c) the steps which the Supplier proposes to take to rectify the Default (I applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable);
Rectification Plan process"	the process set out in Clause 10.3.1 to 10.3.4 (Rectification Plan Process);

Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires);
Reimbursable expenses"	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 expense policy current from time to time, but not including: a) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and b) subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;
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"	a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR); b) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably to 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 information derived from any of the above;

Relevant requirements"	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010;
Relevant Tax authority"	HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established;
Reminder Notice"	a notice sent in accordance with Clause 10.5 given by the Supplier to the Buyer providing notification that payment has not been received on time;

Replacement deliverables"	any deliverables which are substantially similar to any of the Deliverable and which the Buyer receives in substitution for any of the Deliverable 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 insurance"	the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form;
"RTI"	Real Time Information;

Satisfaction certificate"	the certificate (materially in the form of the document contained in of Part B of Call-Off Schedule 13 (Implementation Plan and Testing) or as agreed b the Parties where Call-Off Schedule 13 is not used in this Contract) granted by the Buyer when the Supplier has met all of the requirements of an Order, Achieved a Milestone or a Test;
Security management Plan"	the Supplier's security management plan prepared pursuant to Call- Off Schedule 9 (Security) (if applicable);
Security Policy"	the Buyer's security policy, referred to in the Order Form, in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;
Self-Audit certificate"	means the certificate in the form as set out in Framework Schedule 8 (Self Audit Certificate);
Serious Fraud office"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
Service Levels"	any service levels applicable to the provision of the Deliverables under the Call Off Contract (which, where Call Off Schedule 14 (Service Levels) is used in this Contract, are specified in the Annex to Part A of such Schedule);
Service Period"	has the meaning given to it in the Order Form;

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 ate"	the date of a Service Transfer;
Sites"	any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or b) the Supplier manages, organizes or otherwise directs the provision or the use of the Deliverables;
SME"	an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium enterprises;
Special Terms"	any additional Clauses set out in the Framework Award Form or Order Form which shall form part of the respective Contract;
Specific Change in aw"	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 Specifi Change in Law on the Deliverables is not reasonably foreseeable at the Start Date;
Specification"	the specification set out in Framework Schedule 1 (Specification), as may, in relation to a Call-Off Contract, be supplemented by the Order Form;

Standards"	any: a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organization for Standardization or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with; b) standards detailed in the specification in Schedule 1 (Specification); c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time; d) relevant Government codes of practice and guidance applicable from time to time;
Start Date"	in the case of the Framework Contract, the date specified on the Framework Award Form, and in the case of a Call-Off Contract, the date specified in the Order Form;

Statement of requirements"	a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Call-Off Procedure;
Storage Media"	the part of any device that is capable of storing and retrieving data;

Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than a Call-Off Contract or the Framework Contract, pursuant to which a third party: a) provides the Deliverables (or any part of them); b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
Sub processor"	any third Party appointed to process Personal Data on behalf of that Processor related to a Contract;
Supplier"	the person, firm or company identified in the Framework Award Form;
Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Call-Off Contract but excluding the Buyer Assets;
Supplier Authorised representative"	the representative appointed by the Supplier named in the Framework Award Form, or later defined in a Call-Off Contract;
Supplier's confidential information"	a) any information, however, it is conveyed, that relates to the busines affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier; b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the

	Supplier's attention or into the Supplier's possession in connection with a Contract; c) Information derived from any of (a) and (b) above;
"Supplier's Contract Manager	the person identified in the Order Form appointed by the Supplier t oversee the operation of the Call-Off Contract and any alternativ 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, plan materials and such other items supplied and used by the Supplier (but no hired, leased or loaned from the Buyer) in the performance of its obligations under this Call-Off Contract;
Supplier Marketing contact"	shall be the person identified in the Framework Award Form;

Supplier non-performance"	where the Supplier has failed to: a) Achieve a Milestone by its Milestone Date; b) provide the Goods and/or Services in accordance with the Service Levels; and/or c) comply with an obligation under a Contract;
Supplier Profit"	in relation to a period, the difference between the total Charges (in nomina cash flow terms but excluding any Deductions) and total Costs (in nomina cash flow terms) in respect of a Call-Off Contract for the relevant period;

Supplier Profit margin"	in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;
Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;
Supporting documentation"	sufficient information in writing to enable the Buyer to reasonably asses 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 governme or municipal charges, duties, imports, contributions. levies or liabilities (oth 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 an of the above, in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction;
Termination Notice"	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate a Contract on a specified date and setting out the grounds for termination;

Test Issue"	any variance or non-conformity of the Deliverables from them requirements as set out in a Call-Off Contract;
Test Plan"	a plan: a) for the Testing of the Deliverables; and b) setting out other agreed criteria related to the achievement of Milestones;

Tests "	any tests required to be carried out pursuant to a Call-Off Contract as set out in the Test Plan or elsewhere in a Call-Off Contract and "**Tested**" and "**Testing**" shall be construed accordingly;
Third Party IPR"	Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
Transferring supplier Employees"	those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;
Transparency information"	the Transparency Reports and the content of a Contract, including an changes to this Contract agreed from time to time, except for – (i) any information which is exempt from disclosure in accordanc with the provisions of the FOIA, which shall be determined by th Relevant Authority; and (ii) Commercially Sensitive Information;
Transparency reports"	the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Call-Off Schedule 1 (Transparency Reports);
"TUPE"	Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other regulations or UK legislation implementing the Acquired Rights Directive

"United Kingdom"	the country that consists of England, Scotland, Wales, and Northern Ireland
Variation"	any change to a Contract;
Variation Form"	the form set out in Joint Schedule 2 (Variation Form);
Variation Procedure"	the procedure set out in Clause 24 (Changing the contract);
VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
VCSE"	a non-governmental organization that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy- note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables;
Working Day"	any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form;

Workday"	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)

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: • **[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.

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 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 favorable 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 principal’s 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.

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 endeavors 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.

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.

ANNEX: REQUIRED INSURANCES

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

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

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

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

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

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	18/09/2025	Refer to call of schedule 5 (Pricing details)	60 months

Joint Schedule 5 (Corporate Social Responsibility)

Definitions

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

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

1. What we expect from our Suppliers

1.1 In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviors 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 victimization 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 Labor and Inhumane Treatment

3.1 The Supplier shall fully cooperate with the appointed independent monitoring organization (which is subject to change at the sole discretion of the Authority) to monitor the rights of workers in electronics supply chains.

3.1.1 The current monitoring organization is: - Electronics Watch a not-for-profit non-governmental organization incorporated under Dutch law (No. 62721445 in the Dutch Chamber of Commerce Trade Register). Electronics Watch

3.2 For any hardware procured through this Framework Agreement RM6098, the Supplier shall disclose in the prescribed format (see Annex 1) details of its First Tier and/or Second Tier and/or Third Tier supply chains (including country and

city factory locations). The Authority will provide this information to Electronics Watch to ensure supply chain labor conditions can be assessed.

3.3 The Supplier:

3.3.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labor;

3.3.2 shall not require any Supplier Staff or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;

3.3.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.

3.3.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offences anywhere around the world.

3.3.5 shall make reasonable enquiries to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offences anywhere around the world.

3.3.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;

3.3.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;

3.3.8 shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;

3.3.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;

3.3.10 shall not use or allow child or slave labor to be used by its Subcontractors;

3.3.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

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

4. Income Security

4.1 The Supplier shall:

4.1.1 ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;

4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

4.1.3 not make deductions from wages:

(a) as a disciplinary measure

(b) except where permitted by law; or

(c) without expressed permission of the worker concerned;

4.1.4 record all disciplinary measures taken against Supplier Staff; and

4.1.5 ensure that Supplier Staff are engaged under a recognized employment relationship established through national law and practice.

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

Signed by [CCS/Buyer]		Date:	

Joint Schedule 11 (Processing Data) – Not Applicable

UK GDPR Information

Data Protection

The Parties acknowledge that for the purposes of Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor. The only processing that the Processor is authorised to do is listed in Annex 1 by the Controller and may not be determined by the Processor. The term “processing” and any associated terms are to be read in accordance with Article 4 of the UK GDPR.

The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe Data Protection Legislation.

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 systematic description of the envisaged processing operations and the purpose of the processing; an assessment of the necessity and proportionality of the processing operations in relation to the Services; an assessment of the risks to the rights and freedoms of Data Subjects; and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data. The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Call-Off Contract:
process that Personal Data only in accordance with Annex 1, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law; ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject. In the event of the Controller reasonably

rejecting Protective Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take account of the:

nature of the data to be protected; harm that might result from a Data Loss Event;

state of technological development; and cost of implementing any measures; ensure that: the Processor Personnel do not process Personal Data except in accordance with this Call-Off Contract (and in particular Annex 1); 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: are aware of and comply with the Processor's duties under this clause; are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor; 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 this Call-Off Contract; and have undergone adequate training in the use, care, protection and handling of Personal Data; and not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

the destination country has been recognized as adequate by the UK government in accordance with Article 45 UK GDPR or section 74 of the DPA 2018; the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 DPA 2018) as determined by the Controller; the Data Subject has enforceable rights and effective legal remedies;

the Processor complies with its obligations under Data Protection Legislation by providing an appropriate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavors to assist the Controller in meeting its obligations); and the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Call-Off Contract unless the Processor is required by Law to retain the Personal Data.

The Processor acknowledges that the Controller must (in accordance with UK GDPR Article 33) without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify a Personal Data Breach to the Information Commissioner's Office, unless the Personal Data Breach is unlikely to result in a risk

to the rights and freedoms of natural persons and where such notification is not made within 72 hours, it must be accompanied by reasons for the delay. In order to enable the Controller to comply with UK GDPR Article 33, subject to clause 1.6, the Processor shall notify the Controller immediately if it:

receives a Data Subject Request (or purported Data Subject Request); receives a request to rectify, block or erase any Personal Data; receives any other request, complaint or communication relating to either Party's obligations under Data Protection Legislation; receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Call-Off Contract; 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 becomes aware of a Data Loss Event. The Processor's obligation to notify under clause 1.5 shall include the provision of further information to the Controller, as details become available. Considering the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including but not limited to promptly providing:

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

such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in Data Protection Legislation; the Controller, at its request, with any Personal Data it holds in relation to a Data Subject; assistance as requested by the Controller following any Data Loss Event; 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. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless: the Controller determines that the processing is not occasional;

the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subject. The Processor shall allow for audits of its Personal Data processing activity by the Controller or

the Controller's designated auditor. Each Party shall designate its own data protection officer if required by Data Protection Legislation. Before allowing any Sub-processor to process any Personal Data related to this Call-Off Contract, the Processor must: notify the Controller in writing of the intended Sub-processor and processing; obtain the written consent of the Controller; enter into a written agreement with the Sub-processor which give effect to the terms set out in this Schedule 7 Clause 1 such that they apply to the Sub-processor; and; provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require. Those Sub-processors approved as at the commencement of this Call-Off Contract are as set out in Annex 1. The Processor must list all approved Sub-processors in Annex 1 and include their name and location and the contact information for the person responsible for privacy and data protection compliance. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors so that the Controller can reject or approve such changes.

The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may upon giving the Processor not less than 30 working days' notice to the Processor amend this Call-Off Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Annex 1 - Processing, Personal Data and Data Subjects

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

The contact details of the Controller's Data Protection Officer are: [redacted]

The contact details of the Processor's Data Protection Officer are: [redacted]

The Processor shall comply with any further written instructions with respect to Processing by the Controller. Any such further instructions shall be incorporated into this Schedule.

Description	Details

Identity of the Controller and Processor	The Parties acknowledge that for the purposes of Data Protection Legislation, the Buyer is the Controller, and the Supplier is the Processor. The only processing that the Processor is authorised to do is listed in Annex 1 by the Controller and may not be determined by the Processor. The term "processing" and any associated terms are to be read in accordance with Article 4 of the UK GDPR.
Subject matter of the Processing	Not used
Duration of the processing	The processing will be undertaken for the duration of the Contract.

Nature and purposes of the processing	Not Applicable
Type of Personal Data being Processed	Not Applicable
Categories of Data Subject	Not Applicable
Locations at which the Supplier and/or its Sub-processors process Personal Data under this Contract and international transfers and legal gateway	Not Applicable

Plan for return and destruction of the data once the processing is complete	Not Applicable

Annex 2 – Security

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

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

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

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

End User Devices e.g.

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

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

Networking e.g. The Supplier shall ensure that any Authority/Buyer Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

Personnel Security e.g. All Supplier Personnel shall be subject to a pre- employment

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

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

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

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

Location of Authority/Buyer Data e.g. The Supplier shall not, and shall procure that none

of its Sub-contractors, process Authority/Buyer Data outside the EEA without the prior written consent of the Authority/Buyer and the Supplier shall not change where it or any of its Sub-contractor's process Authority/Buyer Data without the Authority/Buyer's prior written consent which may be subject to conditions.

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

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

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

- NCSC "Security Design Principles for Digital Services"
- NCSC "Bulk Data Principles"
- NSCS "Cloud Security Principles"

Annex 3 - Joint Controller Agreement-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 3 (Joint Controller Agreement) in replacement of paragraphs 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 18-28 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Relevant Authority]:

i. is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

ii. 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;

iii. is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

iv. is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the

Deliverables where consent is the relevant legal basis for that Processing; and

v. 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 endeavors 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] month on:

(i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

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

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(I) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the

Deliverables and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorized or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorized or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their duties under this Annex 3 (Joint Controller Agreement) and those in respect of Confidential Information;

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where that Party would not be permitted to do so; and

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

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

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

(j) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

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

3. **Data Protection Breach**

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

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

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Data Loss Event and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Data Loss Event;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Data Loss Event; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Data Loss Event, with complete information relating to the Data Loss Event, including, without limitation, the information set out in Clause 3.2.

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

(a) the nature of the Data Loss Event;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Data Loss Event; and

(f) describe the likely consequences of the Data Loss Event.

4. **Audit**

4.1 The Supplier shall permit:

(a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 3 and the Data Protection Legislation; and/or

(b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide

evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. **Impact Assessments**

5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. **ICO Guidance**

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

7. **Liabilities for Data Protection Breach**

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

7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Data Loss Event ("**Financial Penalties**") then

the following shall occur:

(a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Data Loss Event, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost, when necessary, an independent third party to conduct an audit of any such Data Loss Event. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Data Loss Event;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Data Loss Event, in that it is not a Data Loss Event that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of

such Data Loss Event; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Data Loss Event and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Data Loss Event can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Data Loss Event, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Data Loss Event shall be liable for the losses arising from such Data Loss Event. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Data Loss Event (the "Claim Losses"):

(a) if the Relevant Authority is responsible for the relevant Data Loss Event, then the Relevant Authority shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Data Loss Event, then the Supplier shall be responsible for the Claim Losses: and

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

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

8. **Termination**

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

9. **Sub-Processing**

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

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. **Data Retention**

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

Call-Off Schedule 1 (Transparency Reports)

1.1 The Supplier recognizes 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.

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
Statement of Work	Migration Plan to assist Buyer's own installation team	Written statement	Once shortly after commencement of the Call-Off Contract

Call-Off Schedule 4 (Call Off Tender)

Social value bid submission

Please refer to call off schedule 5 for commercial bid submission.

Call-Off Schedule 5 (Pricing Details)

[redacted]

	TOTAL COST OF OWNERSHIP FOR 60 MONTHS EX VAT	£367,156.65						

Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements

1. Definitions

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

"Breach of Security"	**1 the occurrence of:** a) **any unauthorized access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or** b) **the loss and/or unauthorized disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer**

	and/or the Supplier in connection with this Contract, **2 in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;**
"Security Management Plan"	**3 the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.**

2. Complying with security requirements and updates to them

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

2.2 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that

the Security Management Plan produced by the Supplier fully complies with the Security Policy.

2.3 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

2.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

2.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

3.2.4 where specified by the Buyer in accordance with paragraph 2.2

complies with the Security Policy and the ICT Policy.

3.3 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. Security Management Plan

4.1 Introduction

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

4.2 Content of the Security Management Plan

4.2.1 The Security Management Plan shall:

a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;

b) identify the necessary delegated organizational roles for those responsible for ensuring it is complied with by the Supplier;

c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the

Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;

f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and

g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in

this Schedule.

4.3 **Development of the Security Management Plan**

4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavors to ensure that the approval process takes as little time as possible and, in any event, no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However, a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.3.4 Approval by the Buyer of the Security Management Plan pursuant to

Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

4.4 **Amendment of the Security Management Plan**

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

a) emerging changes in Good Industry Practice;

b) any change or proposed change to the Deliverables and/or associated processes;

c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;

d) any new perceived or changed security threats; and

e) any reasonable change in requirements requested by the Buyer.

4.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

a) suggested improvements to the effectiveness of the Security Management Plan;

b) updates to the risk assessments; and

c) suggested improvements in measuring the effectiveness of controls.

4.4.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result

of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

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

5. Security breach

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

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

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

a) minimise the extent of actual or potential harm caused by any Breach of Security;

b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

c) prevent an equivalent breach in the future exploiting the same cause failure; and

d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

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

Part B: Long Form Security Requirements- not used

1. Definitions

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

Breach of Security"	**4 means the occurrence of:** a) **any unauthorized access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or** b) **the loss and/or unauthorized disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,** **5 in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance**

	therewith in accordance with paragraph 3.4.3 d;
"ISMS"	**6 the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and**
"Security Tests"	**7 tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.**

2. Security Requirements

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

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

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

2.3.1 Name:

Email:

Telephone:

2.3.2 Name:

Email:

Telephone:

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

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

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

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

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

3. Information Security Management System (ISMS)

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

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

3.3 The Buyer acknowledges that;

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

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

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

3.4 The ISMS shall:

3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;

3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.3 at all times provide a level of security which:

a) is in accordance with the Law and this Contract;

b) complies with the Baseline Security Requirements;

c) as a minimum demonstrates Good Industry Practice;

d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;

e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) (https://www.gov.uk/government/publications/security- policy-framework/hmg-security-policy-framework)

f) takes account of guidance issued by the Centre for Protection of National Infrastructure (https://www.cpni.gov.uk)

g) complies with HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm)

h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

i) addresses issues of incompatibility with the Supplier's own organizational security policies; and

j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.4 document the security incident management processes and incident

response plans;

3.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritization of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

3.4.6 be certified by (or by a person with the direct delegated authority of)

3.4.7 a

Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

3.5 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

3.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is

Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavors to ensure that the Approval process takes as little time as possible and, in any event, no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However, any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable

Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4. Security Management Plan

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

4.2 The Security Management Plan shall:

4.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);

4.2.2 comply with the Baseline Security Requirements and, where specified

by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;

4.2.3 identify the necessary delegated organizational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;

4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule

(including the requirements set out in Paragraph 3.4);

4.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimized the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non- approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavors to ensure

that the Approval process takes as little time as possible and, in any event, no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However, any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

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

5. Amendment of the ISMS and Security Management Plan

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

5.1.1 emerging changes in Good Industry Practice;

5.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;

5.1.3 any new perceived or changed security threats;

5.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;

5.1.5 any new perceived or changed security threats; and

5.1.6 any reasonable change in requirement requested by the Buyer.

5.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

5.2.1 suggested improvements to the effectiveness of the ISMS;

5.2.2 updates to the risk assessments;

5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.

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

6. Security Testing

6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer.

Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

6.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.

6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against

any resultant under- performance for the period of the Buyer's test.

6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un- patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. Complying with the ISMS

7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.

7.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time, then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.

7.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of

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

8. Security Breach

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

8.2 Without prejudice to the security incident management process, upon becoming

aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

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

a) minimise the extent of actual or potential harm caused by any Breach of Security;

b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;

c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are

reasonably related to a possible incident or compromise); and

f) as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

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

9. Vulnerabilities and fixing them

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

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

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

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

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

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

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

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

9.4 The Specification and Mobilization Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

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

9.4.2 is agreed with the Buyer in writing.

9.5 The Supplier shall:

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

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

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

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

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

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

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

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

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

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

Part B – Annex 1:

Baseline security requirements

1. Handling Classified information

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

2. End user devices

2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognized certification process of the National Cyber Security Centre (“NCSC”) to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").

2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a ‘known good’ state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (https://www.ncsc.gov.uk/guidance/end- user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis

with the Buyer.

3. Data Processing, Storage, Management and Destruction

3.1 The Supplier and Buyer recognize the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

3.3 The Supplier shall:

3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has

been formally assured through a certification process recognized by NCSC, to at least Foundation Grade, for example, under CPA.

4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. Security by design

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognized security professionals with the appropriate skills and/or a NCSC certification (https://www.ncsc.gov.uk/section/products-services/ncsc-certification) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except were agreed with the Buyer in writing.

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

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

7. Restricting and monitoring access

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

8. Audit

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

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

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

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

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

Call-Off Schedule 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 realized.

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 regard 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.

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-Not used

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 endeavors to ensure that a delegate attends the Operational Board

meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.

4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

5. Contract Risk Management

5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.

5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

5.2.1 the identification and management of risks;

5.2.2 the identification and management of issues; and

5.2.3 monitoring and controlling project plans.

5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

5.4 The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer's and the Supplier have identified.

Call-Off Schedule 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

[redacted]

	TOTAL COST OF OWNERSHIP FOR 60 MONTHS EX VAT	£387,156.65

Appendix 1
CLOUDIAN END USER LICENSE AGREEMENT

This Cloudian End User License Agreement (this "**Agreement**") is an agreement between Cloudian, Inc., a Delaware corporation ("**Cloudian**") and the company identified by you on this page ("**Licensee**"). IT IS IMPORTANT THAT YOU READ THIS AGREEMENT CAREFULLY AND COMPLETELY. THIS AGREEMENT IS A LEGALLY BINDING AGREEMENT BETWEEN CLOUDIAN AND LICENSEE. BY CHECKING THE "I HAVE READ AND AGREE TO THE AGREEMENT" BOX AND/OR CLICKING THE "SUBMIT" BUTTON ON THIS PAGE BY DOWNLOADING OR INSTALLING ANY CLOUDIAN SOFTWARE, OR BY INSTALLING ANY CLOUDIAN LICENSE KEY OR USING ANY CLOUDIAN PRODUCT IN ANY MANNER, YOU ARE BINDING LICENSEE TO THE TERMS OF THIS AGREEMENT, AND YOU ARE REPRESENTING TO CLOUDIAN THAT YOU ARE DULY AUTHORIZED BY LICENSEE TO DO SO AND THAT LICENSEE IS A CORPORATION OR OTHER BUSINESS ENTITY. IF LICENSEE IS NOT A CORPORATION OR OTHER BUSINESS ENTITY, IF YOU ARE NOT AUTHORIZED TO BIND LICENSEE TO THE TERMS OF THIS AGREEMENT, OR IF LICENSEE DOES NOT AGREE TO BE BOUND BY ALL OF THE TERMS OF THIS AGREEMENT, DO NOT CHECK THE "I HAVE READ AND AGREE TO THE AGREEMENT" BOX, DO NOT CLICK THE "SUBMIT" BUTTON, DO NOT DOWNLOAD OR INSTALL ANY CLOUDIAN SOFTWARE, DO NOT INSTALL ANY CLOUDIAN LICENSE KEYS, AND DO NOT USE ANY CLOUDIAN PRODUCT IN ANY MANNER. IF LICENSEE DOES NOT AGREE TO BE BOUND BY ALL OF THE TERMS OF THIS AGREEMENT, THE CLOUDIAN PRODUCT MAY BE RETURNED TO THE SELLER FOR A REFUND OF THE PURCHASE PRICE ACTUALLY PAID BY LICENSEE.

1. DEFINITIONS

1.1 "Cloudian Product" means any Cloudian product for which Cloudian provides to Licensee one or more license keys. "Cloudian Software Product" means any Cloudian Product that is a software- only product (with no hardware), and "Cloudian Appliance Product" means any Cloudian Product that is an appliance product.

1.2 "Cloudian-Powered Storage System" means an object storage system with a single shared namespace. The nodes of such system may be distributed across multiple data centers in multiple geographic regions.

1.3 "Documentation" means, with respect to a Cloudian Product, Cloudian's standard end-user manuals for such Cloudian Product and any updates thereto that may be provided by Cloudian or Seller (if Seller is not Cloudian) to Licensee.

1.4 "Evaluation License Term" means, with respect to an Evaluation License, the license period encoded in the evaluation license key provided by Cloudian to Licensee for such Evaluation License; provided, however, that if, prior to the end of such period, a production license key is installed on any node of the Cloudian-Powered Storage System covered by such evaluation license key, the Evaluation License Term will terminate upon such installation of such production license key. For avoidance of doubt, there will be no Evaluation License Term for any Cloudian Product unless and until an evaluation license key is provided by Cloudian to Licensee for such Cloudian Product.

1.5 "Licensed Software" means (a) with respect to a Cloudian Software Product, such Cloudian Software Product and all corrections, updates and upgrades thereto that Cloudian or Seller (if Seller is

not Cloudian) may provide to Licensee, and (b) with respect to a Cloudian Appliance Product unit, (i) the software installed on such unit at the time it is originally delivered to Licensee ("Preloaded Licensed Software"), (ii) any other software that Cloudian or Seller (if Seller is not Cloudian) may provide to Licensee for use with such product ("Non-Preloaded Licensed Software"), and (iii) any corrections, updates and upgrades to any of the foregoing that Cloudian or Seller (if Seller is not Cloudian) may provide to Licensee.

1.6 "Licensed Storage Amount" means, with respect to a Software License, the maximum amount of storage permitted for such Software License (which may be measured by the total data storage capacity of all storage devices that can be accessed by the applicable Cloudian Product, the amount of storage space configured for use by such Cloudian Product, or another metric defined by Cloudian), as encoded in the license key for such Software License.

1.7 "Permitted Purposes" means (a) with respect to an Evaluation License, the testing and evaluation of the applicable Cloudian Product in a non-production capacity, and (b) with respect to a Production License, Licensee's internal business purposes.

1.8 "Production License Term" means, with respect to a Production License, the license period encoded in the production license key provided by Cloudian to Licensee for such Production License; provided that the Production License Term of each Production License for Licensed Software for a Cloudian Appliance Product will have a perpetual duration.

1.9 "Seller" means, with respect to a Cloudian Product, the entity from which such Cloudian Product is obtained by Licensee.

1.10 "Software License" means a license granted by Cloudian to Licensee under Section 2.1 in connection with a license key provided by Cloudian to Licensee. A Software License is an "Evaluation License" if the corresponding license key is an evaluation license key, and a "Production License" if the corresponding license key is a production license key.

1.11 "Third PartySoftware" means any software not developed by Cloudian that may be provided by Cloudian to Licensee together with separate license terms that govern such software.

2. LICENSE GRANTS

2.1 Licensed Software. Subject to the terms and conditions of this Agreement (including Section 3), Cloudian hereby grants to Licensee, with respect to each license key, a non-exclusive, non-transferable (except as permitted in Section 12.3), non-sublicensable license to do all of the following during the license period (i.e., the Evaluation License Term or Production License Term) encoded in such license key: (a) if such license key is for a Cloudian Software Product, install and use such Cloudian Software Product to operate a single Cloudian-Powered Storage System solely for Permitted Purposes, subject to the applicable Licensed Storage Amount; or (b) if such license key is for a Cloudian Appliance Product unit, install the Non-Preloaded Licensed Software for such Cloudian Appliance Product, if any, on such unit, and use the Licensed Software on such unit solely for Permitted Purposes, subject to the applicable Licensed Storage Amount. Notwithstanding the foregoing, this Section does not apply to any Third Party Software, all of which is provided to Licensee pursuant to separate licensing terms.

2.2 Documentation. Subject to the terms and conditions of this Agreement (including Section 3), Cloudian hereby grants to Licensee a non-exclusive, non-transferable (except as permitted in Section 12.3), non-sublicensable license to do the following during the license period (i.e., the Evaluation License Term or Production License Term) of each Software License: make and use a reasonable number of copies of the Documentation for the applicable Cloudian Product solely in connection with the permitted use thereof.

3. SOFTWARE RESTRICTIONS

3.1 Appliance-Specific Restrictions. The Licensed Software for each Cloudian Appliance Product unit is licensed for use solely on the hardware of such unit. Licensee will not, and will have no right to: (a) move such Licensed Software to, or otherwise install or use such Licensed Software on, any hardware other than the hardware of such unit; or (b) use such Licensed Software if the storage capacity of such unit is expanded beyond what was originally delivered to Licensee (including through the addition of storage devices to, or the upgrading of the storage devices of, such unit). Prior to selling, leasing or otherwise transferring any Cloudian Appliance Product unit to any third party, Licensee will permanently delete all Licensed Software installed on such unit.

3.2 Other Restrictions. Licensee will not, and will have no right to, do any of the following: (a) install, use or copy any Licensed Software or Documentation except as permitted in Section 2; (b) without limitation of the foregoing, use any Licensed Software or Documentation in connection with the development, marketing, distribution or exploitation of any products or services that are competitive with any Licensed Software or Cloudian Product, or use any Licensed Software or Cloudian Product under an Evaluation License in a production capacity; (c) distribute, disclose or otherwise provide any Licensed Software or Documentation to any third party; (d) grant to any third party any license, sublicense or other rights in or to, or otherwise permit any third party (other than Licensee's contractors acting on behalf of Licensee during any Production License Term) to use, any Licensed Software or Documentation (for avoidance of doubt, this subsection (d) does not prohibit or limit use by third parties of any storage service operated by Licensee using the Licensed Software during any Production License Period); (e) create derivative works of, translate, adapt or otherwise modify any Licensed Software or Documentation; (f) decompile, disassemble or reverse engineer any Licensed Software, or otherwise attempt to derive or extract any source code, ideas, algorithms, procedures, workflows or hierarchies from any Licensed Software; (g) disclose the results of any performance tests, or any benchmark tests or other comparative analyses, of any Licensed Software or Cloudian Products; (h) disclose the specifications of, or Cloudian's roadmap for, any Licensed Software or Cloudian Product to any third party; or (i) authorize, instruct or assist any third party to perform any of the foregoing activities. Licensee will comply with all applicable laws (including consumer, privacy and telecommunications laws) in connection with all activities involving any Licensed Software or Cloudian Product.

3.3 Injunctive Relief. Licensee acknowledges and agrees that any breach of Sections 3.1 or 3.2 by Licensee will cause irreparable injury to Cloudian and that, in addition to any other remedies that may be available to Cloudian, Cloudian will be entitled to obtain injunctive relief against such breach or threatened breach or the continuation of such breach, without any requirement to prove actual damages or post a bond or other security.

3.4 Enforcement Mechanisms. Licensee acknowledges and agrees that (a) Licensed Software will only operate on servers on which valid license keys are installed and (b) Licensed Software may contain

certain other mechanisms to enforce the Licensed Storage Amount limitation and the other limitations set forth in this Agreement. Cloudian will have no liability of any kind in connection with any inability of Licensee to use the Licensed Software or the Cloudian Product in excess of such limitations due to such mechanisms or any other causes.

3.5 Export restrictions. Licensee acknowledges that Licensed Software and Cloudian Products are subject to U.S. and foreign customs and export control laws and regulations (collectively, "Export Laws"). Licensee will comply with Export Laws, and Licensee will be solely responsible for obtaining any necessary licenses or other authorizations relating to the export of Licensed Software or Cloudian Products. Without limitation of the foregoing, Licensee will not import, export, re-export, sell or otherwise transfer any Licensed Software or Cloudian Product (a) to restricted end-users or to restricted countries (as defined by the Export Laws), or (b) for the design, development, production or use of nuclear weapons, materials or facilities, chemical or biological weapons, or missile technology, or for any other purposes prohibited by Export Laws.

3.6 Records; Audit. Licensee will keep and maintain complete and accurate books and records relating to this Agreement, and Cloudian will have the right, from time to time and with reasonable advance notice to Licensee, to conduct an audit of Licensee's books and records and Licensee's use of Licensed Software to verify Licensee's compliance with the terms and conditions of this Agreement. No such audit will unreasonably interfere with Licensee's business activities. If any such audit reveals any material breach of this Agreement, Licensee will promptly pay to Cloudian all costs and expenses of such audit. Without prejudice to any other rights of Cloudian, Licensee will promptly pay Cloudian the amount of any underpayment by Licensee, and correct any other noncompliance, revealed by any such audit.

3.7 Software Data Usage Files. The Licensed Software may generate electronic files containing information regarding its usage ("Audit Files"). Upon any request by Cloudian, Licensee will promptly generate and send to Cloudian Audit Files any other reports or logs that can be generated by the Licensed Software (such reports and logs, collectively with Audit Files, "Software Usage Data Files"), or, at Cloudian's option, permit and enable Cloudian to remotely generate Software Usage Data Files and retrieve them over the Internet.

3.8 NVIDIA Components. The Licensed Software includes certain NVIDIA software libraries and related materials (the "NVIDIA Components"). NVIDIA Components are licensed, not sold, and remain the property of NVIDIA Corporation and its licensors. Licensee may use the NVIDIA Components solely as incorporated into the Licensed Software and only in systems that include NVIDIA GPUs, NVIDIA CPUs, or NVIDIA (Mellanox) networking cards, with RDMA functionality requiring the presence of an NVIDIA (Mellanox) networking card and not operating on non-Mellanox interfaces. Licensee receives no rights to use the NVIDIA Components on a standalone basis and may not copy, distribute, sublicense, or otherwise make them available except as part of the Licensed Software. The NVIDIA Components are provided "AS IS" and with all faults, and Cloudian disclaims all warranties and conditions, express, implied, or statutory, including without limitation implied warranties of merchantability, fitness for a particular purpose, and non-infringement. The NVIDIA Components are not intended for mission-critical applications, meaning uses where failure could cause injury, loss of life, or severe damage, and Licensee assumes responsibility for any such use.

4. EVALUATION HARDWARE RESTRICTIONS

Licensee will not (a) remove any hardware from, add any hardware to, or modify any hardware of, any Cloudian Appliance Product unit that is provided to Licensee for evaluation purposes, except that Licensee may remove hardware components from such unit on a temporary basis solely for failure testing purposes, or (b) distribute, disclose or otherwise provide any portion of such Cloudian Appliance Product unit to any third party. Cloudian will retain title to and ownership of any Cloudian Appliance Product unit that is provided to Licensee for evaluation purposes unless and until Licensee purchases such unit from Cloudian.

5. SUPPORT

5.1 Support Agreement. With respect to any technical support services for Cloudian Products purchased by Licensee, Licensee agrees that if such technical support is to be provided to Licensee directly by Cloudian, it will be governed by Cloudian's technical support terms located at cloudian.com/disclosures/technical-support-terms, and if it is to be provided to Licensee by a Cloudian reseller or distributor, it will be governed by terms agreed to between Licensee and such reseller or distributor. Cloudian will have no obligation under this Agreement to provide any technical support or maintenance for, or any bug fixes, updates or upgrades to, any Cloudian Product or Licensed Software.

5.2 Support Diagnostics. Cloudian may collect product usage data, log files, trace files, and other usage and diagnostic data (collectively, "Diagnostic Data") from each Cloudian Product, which collection may be achieved using "call home" functionality of such Cloudian Product or through manual collection from such Cloudian Product (Licensee may choose the collection method). Cloudian and its business partners may use Diagnostic Data to provide, support and enhance Cloudian's products and services. Cloudian may also use Diagnostic Data to determine usage trends for Cloudian Products and Licensed Software, and Cloudian may publicly disclose such trends as long as Licensee is not identified by name as a source of Diagnostic Data.

5.3 Remote support capabilities. Licensee will give Cloudian reasonable notice before removing or disabling any remote support capabilities of any Cloudian Product during any technical support term.

6. PROMOTIONAL CONSIDERATION

6.1 Cloudian will have the right to use Licensee's name and logo to identify Licensee as a user of Cloudian Products on Cloudian's websites and promotional materials until Licensee expressly objects in writing.

7. PROPRIETARY RIGHTS

7.1 Ownership. Licensee acknowledges and agrees that, as between Cloudian and Licensee, Cloudian and/or its licensors own and will retain all right, title and interest (including all intellectual property rights) in and to all Licensed Software and Documentation. If Licensee provides Cloudian with any feedback (including any ideas or suggestions for new features or other improvements) regarding any Cloudian Product, Cloudian will be free to implement and otherwise use such feedback for any purpose, without restriction and without compensation or attribution to Licensee.

7.2 No implied rights. Except as expressly set forth in this Agreement, Cloudian grants no licenses or other rights in or to any Licensed Software or Documentation (whether by implication, estoppel, or otherwise) to Licensee or any third parties. All rights not expressly granted to Licensee are retained by Cloudian and its licensors.

7.3 Proprietary rights markings. Licensee will ensure that all copies of Licensed Software and Documentation will contain all copyright, trademark, patent, confidentiality and other notices in the same manner as such notices appear on or in such Licensed Software and Documentation as originally provided to Licensee. Licensee will not remove, alter, cover or obfuscate any such notices placed on or in any Cloudian Product, Licensed Software or Documentation.

8. WARRANTY AND DISCLAIMERS

8.1 Limited warranties

(a) With respect to each Production License, Cloudian warrants to Licensee that, for a period of thirty (30) days commencing on the first day of the applicable Production License Term ("Software Warranty Period"), the Licensed Software covered by such Production License, in the form delivered to Licensee by Cloudian or Seller (if Seller is not Cloudian), will perform substantially in accordance with the functional specifications for such Licensed Software set forth in the applicable Documentation when installed and used in compliance with such Documentation and this Agreement. For the purposes of this Agreement, a Cloudian Software Product will be deemed to be delivered to Licensee when it is made available for download by Licensee. For avoidance of doubt, the foregoing warranty does not apply to any Licensed Software while it is being used under an Evaluation License or during any other period in which it is not covered by a Production License.

(b) With respect to each Cloudian Appliance Product unit purchased by Licensee from Cloudian or Seller (if Seller is not Cloudian), Cloudian warrants to Licensee that, for a period of thirty (30) days commencing on the date of sale of such unit ("Hardware Warranty Period"), the hardware of such Cloudian Appliance Product unit, in the form delivered to Licensee by Cloudian or Seller (if Seller is not Cloudian), will be free of material defects in materials and workmanship under normal use. For avoidance of doubt, the foregoing warranty does not apply to any Cloudian Appliance Product unit that is provided by to Licensee for evaluation purposes unless and until such unit is purchased by Licensee.

8.2 Remedies

(a) If, during the Software Warranty Period applicable to any Production License, Licensee provides Cloudian written notice of any breach of the warranty set forth in Section 8.1(a) above with respect to the Licensed Software covered by such Production License, which notice describes such breach in detail, Cloudian will (at Cloudian's election) either (i) correct such Licensed Software so that it complies with such warranty or (ii) replace such Licensed Software with software that complies with such warrant.

(b) If, during the Hardware Warranty Period applicable to any Cloudian Appliance Product unit, Licensee provides Cloudian written notice of any breach of the warranty set forth in Section 8.1(b) above with respect to such unit, which notice describes such breach in detail, Cloudian will (at Cloudian's election) either (i) repair the defective hardware (using new or previously used parts that

are equivalent to new in performance and reliability) so that it complies with such warranty or (ii) replace the defective hardware (in part or whole) with other hardware that complies with such warranty (such replacement hardware may contain, or consist of, new or previously used parts that are equivalent to new in performance and reliability). In connection with subsections (i) and (ii) above, Cloudian may request that Licensee replace certain user-installable parts. Repaired or replacement hardware will be warranted for the remainder of the original Hardware Warranty Period.

(c) Notwithstanding anything to the contrary, Cloudian will not accept the return of any hardware from Licensee unless Licensee obtains a Return Material Authorization number from Cloudian and such number is included with the return. For any such return, Licensee will prepay the shipping charges and insure the shipment (or accept the risk if the returned items are lost or damaged in shipment). All hardware returned by Licensee to Cloudian will become the property of Cloudian. Licensee will return to Cloudian all defective hardware for which Cloudian provides a replacement to Licensee, and if Licensee does not do so, Licensee will pay Cloudian's then-current spare parts price for such hardware to Cloudian.

(d) This Section 8.2 sets forth Licensee's sole remedy and Cloudian's sole liability for any breach of the warranties set forth in Section 8.1.

8.3 Warranty exclusions. Cloudian will have no liability and no obligations in connection with any breach of any warranty set forth in Section 8.1 if (a) the affected Licensed Software or Cloudian Appliance Product unit is used or installed in a manner that is not consistent with the Documentation or not permitted under this Agreement, (b) such Licensed Software or Cloudian Appliance Product unit is subject to any abuse, misuse, neglect, accident or casualty loss, or to any modification, alteration or repair not performed by Cloudian or its authorized representative, or (c) the original identification marks have been removed from such Licensed Software or Cloudian Appliance Product unit. In addition, Cloudian will have no liability and no obligations in connection with any problems with any Licensed Software or Cloudian Appliance Product unit arising from (i) any third party items or services with which it is used or (ii) any other causes beyond Cloudian's control.

8.4 Disclaimer. EXCEPT FOR THE WARRANTIES SET FORTH IN SECTION 8.1, TO THE EXTENT PERMITTED UNDER APPLICABLE LAW, CLOUDIAN DOES NOT MAKE, AND CLOUDIAN HEREBY DISCLAIMS, ANY REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE) WITH RESPECT TO ANY CLOUDIAN PRODUCT, LICENSED SOFTWARE, DOCUMENTATION OR THIRD PARTY SOFTWARE, OR ANY OTHER PRODUCTS, SERVICES OR MATERIALS PROVIDED BY OR FOR CLOUDIAN HEREUNDER, INCLUDING ANY WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, ACCURACY OR NONINFRINGEMENT, AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE. Without limitation of the foregoing, Cloudian does not represent or warrant that any Cloudian Product, Licensed Software, Documentation or Third Party Software, or any services provided by Cloudian, will meet the requirements of Licensee (even if such requirements are known to Cloudian) or will operate without interruption or be error free, or that any defects in any Cloudian Product or Licensed Software can be corrected. For purposes of clarification, Cloudian makes no representations or warranties to any of customers of Licensee or other third parties.