Crown Commercial Service

Digital Outcomes and Specialists 5 (RM1043.7)

Framework Schedule 6 (Order Form)

Version 2

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

Order Form

Call-Off Reference: WP2114

Call-Off Title: WP2114 GOV.UK Search Site Improvement

Call-Off Contract Description: Identify, test and evaluate a range of managed site search solutions for the GOV.UK website to improve search performance. The chosen solution will be integrated with the GOV.UK tech stack in a subsequent stage of work.

Our goal is to significantly improve the quality of the GOV.UK site search experience for users by improving the relevancy of results. We would also like to reduce the long term maintenance work required of the GOV.UK team.

GOV.UK site search is currently powered by a self-hosted Elasticsearch database. We would like to investigate and evaluate alternative search solutions. We're particularly interested in fully managed search engine services. If we can identify a measurably better solution for users, we want to implement it.

We want to test and evaluate a range of managed site search solutions, to identify the best solution for measurably improving the relevancy of GOV.UK search results. We then want to integrate that solution with the GOV.UK tech stack.

Stage 1: Evaluate & trial Search products

- Work with GOV.UK stakeholders and users to establish functional and non-functional requirements, based around user needs. This will include accessibility requirements (at least WCAG AA) and progressive enhancement

- Work with the stakeholders to establish evaluation criteria

- Create Proof of concepts with selected products

- Develop and implement a comparative quantitative testing approach to make an evidence-based comparison of products with representative usage

- Evaluate and shortlist potential products, to establish the best fit with GOV.UK's requirements and make recommendations for approval by stakeholders

Stage 2: Implementation

- Implement new search approach into GOV.UK's live tech stack

- A/B testing of the new approach as part of staged rollout

- Design process for any search management required by GOV.UK teams

- Outline any developer tasks required on a ongoing basis

Stage 3: Support and optimisation

- Ongoing optimisation of the chosen platform

- Ongoing support and maintenance of the chosen platform

The Buyer: The Cabinet Office

Buyer Address:

- **Main Address**: I Horse Guards Road, London, SW1A 2HQ.
- **Based:** The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS

The Supplier: Kin and Carta UK Limited

Supplier Address: The Spitfire Building, 71 Collier Street, London, England, N1 9BE. United Kingdom

Registration Number: 01897720

DUNS Number: [redacted]

SID4GOV ID: N/A

Applicable Framework Contract

This Order Form is for the provision of the Call-Off Deliverables and dated 13 October 2022.

It's issued under the Framework Contract with the reference number RM1043.7 for the provision of Digital Outcomes and Specialists Deliverables.

The Parties intend that this Call-Off Contract will not, except for the first Statement of Work which shall be executed at the same time that the Call-Off Contract is executed, oblige the Buyer to buy or the Supplier to supply Deliverables.

The Parties agree that when a Buyer seeks further Deliverables from the Supplier under the Call-Off Contract, the Buyer and Supplier will agree and execute a further Statement of Work (in the form of the template set out in Annex 1 to this Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules).

Upon the execution of each Statement of Work it shall become incorporated into the Buyer and Supplier's Call-Off Contract.

Call-Off Lot

Lot 1: Digital Outcomes

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) RM1043.7

3 Framework Special Terms

4 The following Schedules in equal order of precedence:

- Joint Schedules for RM1043.7
    - Joint Schedule 2 (Variation Form)
    - Joint Schedule 3 (Insurance Requirements)
    - Joint Schedule 4 (Commercially Sensitive Information)
    - Joint Schedule 5 (Corporate Social Responsibility)
    - Joint Schedule 10 (Rectification Plan)
    - Joint Schedule 11 (Processing Data)

- Call-Off Schedules for RM1043.7
    - Call-Off Schedule 1 (Transparency Reports)
    - Call-Off Schedule 2 (Staff Transfer)
    - Call-Off Schedule 3 (Continuous Improvement)
    - Call-Off Schedule 5 (Pricing Details and Expenses Policy)
    - Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables)
    - Call-Off Schedule 7 (Key Supplier Staff)
    - Call-Off Schedule 9 (Security)
    - Call-Off Schedule 10 (Exit Management)
    - Call-Off Schedule 13 (Implementation Plan and Testing)
    - Call-Off Schedule 14 (Service Levels and Balanced Scorecard)
    - Call-Off Schedule 20 (Call-Off Specification)
    - Call-Off Schedule 26 (Cyber Essential Scheme)

5 CCS Core Terms (version 3.0.9)

6 Joint Schedule 5 (Corporate Social Responsibility) RM1043.7

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

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

Call-Off Special Terms

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

Not used.

Call-Off Start Date: 06 March 2023

Call-Off Expiry Date: 05 December 2023

Call-Off Initial Period: 9 months. Can be extended to 05 March 2024, subject to CO Approvals.

Call-Off Optional Extension Period: Buyer can request to extend DOS Contract up to 3 month contract, subject to Cabinet Office approvals

Minimum Notice Period for Extensions: Four (4) weeks

Call-Off Contract Value: £778,350 (excluding VAT) for 9 month period from 06 March 2023 - 05 December 2023.

Subject to Cabinet Office approval the Buyer may extend the contract for a further 3 months with Call-Off value of up to £898,000 (excluding VAT).

Call-Off Deliverables

Option B: See details in Call-Off Schedule 20 (Call-Off Specification)

Buyer's Standards

From the Start Date of this Call-Off Contract, the Supplier shall comply with the relevant (and current as of the Call-Off Start Date) Standards referred to in Framework Schedule 1 (Specification). The Buyer requires the Supplier to comply with the following additional Standards for this Call-Off Contract:

The Supplier should follow where applicable:

- The Government Technology Code of Practice (https://www.gov.uk/government/publications/technology-code-of-practice)
- The Government Service Standard and Service Manual (https://www.gov.uk/service-manual/service-standard)
- Resources to be supplied in accordance with DDAT Competency framework guidelines: https://www.gov.uk/government/collections/digital-data-and-technology-profession-capability-framework
- NCSC Cyber Assessment Framework Guidance https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework
- NCSC guidance https://www.ncsc.gov.uk/section/advice-guidance/all-topics
- Minimum Cyber Security Standards https://www.gov.uk/government/publications/the-minimum-cyber-security-standard/the-minimum-cyber-security-standard
- NCSC Cloud Security Principles https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles
- ISO 270001

Cyber Essentials Scheme

The Buyer requires the Supplier, in accordance with Call-Off Schedule 26 (Cyber Essentials Scheme) to provide a Cyber Essentials Certificate prior to commencing the provision of any Deliverables under this Call-Off Contract.

Maximum Liability

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

as amended by the Framework Award Form Special Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £778,350 (excluding VAT).

Call-Off Charges

1 Capped Time and Materials (CTM)

Where non-UK Supplier Staff (including Subcontractors) are used to provide any element of the Deliverables under this Call-Off Contract, the applicable rate card(s) shall be incorporated into Call-Off Schedule 5 (Pricing Details and Expenses Policy) and the Supplier shall, under each SOW, charge the Buyer a rate no greater than those set out in the applicable rate card for the Supplier Staff undertaking that element of work on the Deliverables.

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Specific Change in Law

Reimbursable Expenses

See Expenses Policy in Call-Off Schedule 5 (Pricing Details and Expenses Policy) and Annex 3 of 'WP2103 User Research Participants for GOV.UK Roadmap: DOS5 Schedule 6 Order Form'.

Payment Method

Invoice to be emailed monthly in arrears.

[redacted]

Buyer's Invoice Address

Name: [redacted]

Role: Paying invoices on behalf of Cabinet Office

Phone:

Email Address: [redacted]

Address: SSCL: Shared Services Connected Ltd Sortation Ref 601 Phoenix House Newport NP10 8FZ.

Cabinet Office:

Main Address: I Horse Guards Road, London, SW1A 2HQ.
Based: The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS

Buyer's Authorised Representative

[redacted]

[redacted]

Address: The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS

[redacted]

Address: The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS

Buyer's Environmental Policy

Cabinet Office Environment policy, available at request. Please email GDS Commissioning Team [redacted]

Buyer's Security Policy

Cabinet Office Security Breach Policy, Physical Security Policy and Personnel Vetting Policy, all available on request. Please email GDS Commissioning Team [redacted]

Supplier's Authorised Representative

[redacted]

Address: The Spitfire Building, 71 Collier Street, London, England, N1 9BE. United Kingdom

Supplier's Contract Manager

[redacted]

Address: The Spitfire Building, 71 Collier Street, London, England, N1 9BE. United Kingdom.

Progress Report Frequency

Progress Report to be provided on a monthly basis when there are commissions under way.

Progress Meeting Frequency

Progress Meeting to be held on a monthly basis when there are commissions under way.

Key Staff

[redacted]

Supplier anticipates two additional roles to be added to the Project under this Order Form under Call-Off WP2114. The initial phase of the Project will define the scope for these potential two additional roles and a subsequent amendment shall be issued should they be added as part of the Project hereto.

[redacted]

The Contracting Authority deems this a Contracted out service: the off-payroll rules do not apply.

Key Subcontractor(s)

[redacted]

Commercially Sensitive Information

Any information relating to: Personal information (CV's, contact details etc.); pricing and details of Supplier's cost base; insurance arrangements; proprietary information; and/or approach and/or methodologies, is commercially sensitive/confidential and exempt from disclosure under the Freedom of Information Act 2000 ("FOIA"). If a request to disclose such information is received, the Parties will work together and consider the applicability of any FOIA exemptions.

BALANCED SCORECARD

See Call-Off Schedule 14 (Service Levels and Balanced Scorecard)

Material KPIs

The following Material KPIs shall apply to this Call-Off Contract in accordance with Call-Off Schedule 14B (Service Levels and Balanced Scorecard):

A. KPI: Performance to pay process

Met	**Partially met**	**Not met**
All of the inputs are submitted in accordance with the performance to pay process timescales and contain accurate and complete information	Inputs are later than prescribed in the performance to pay process but within 5 working days of the prescribed dates • Inputs are incomplete or inaccurate	Inputs are later than 5 working days in the prescribed performance to pay process Inputs contain significant errors

B. KPI: People (resourcing)

Met	**Partially met**	**Not met**
Targets met for all resources or facilities	Targets met for most (50%+) resources or facilities through no fault of the Buyer	Targets missed for most resources or facilities requested through no fault of the Buyer

C. KPI: Partnering behaviours and added value

Met	**Partially met**	**Not met**

• No behavioural problems identified • Buyer workshops attended and positive contributions made • Added value recognised by the programme above provision of compensated skilled resource/facilities	• Some minor behavioural problems • Supplier only attends some workshops or provides minor contributions • Supplier adds some value above provision of compensated resource and facilities, but this is not regarded as significant	• Significant behavioural problems • Supplier contributions are rare or insignificant and shows little interest in working with other suppliers • No added value contributions recognised by the Programme

D.KPI: People in place (Delivery)

Met	**Partially met**	**Not met**
• No resources are swapped out due to deficiency in skill-set and/or no change of facilities is required • No problems identified with quality of work or state of facility • Supplier is making positive team contributions • Supplier skills or	• Minor issues noted with quality of work or standard of facilities • Few contributions made within team	• Resource is swapped out from project due to deficiency in skill-set or change of facility is required • Persistent issues with quality of work or facilities noted (may be minor ones which have persisted from one month to

facilities meet the standards expected		another) • Significant issue with quality of work or facility noted in a month

Additional Insurances

Not applicable

Guarantee

Not applicable

Social Value Commitment

Not applicable

Statement of Works

During the Call-Off Contract Period, the Buyer and Supplier may agree and execute completed Statement of Works. Upon execution of a Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

For and on behalf of the Supplier: Kin and Carta UK Limited

Signature:

DocuSigned by:
David Tuck
36213A7392F449B...

Name: [redacted]

Role: [redacted]

Date: 23 February 2023

For and on behalf of the Buyer: Cabinet Office

Signature:

Name: Role: Date:

[redacted]

[redacted]

22nd February 2023

Appendix 1

Statement of Works (SOW) Details

Upon execution, this SOW forms part of the Call-Off Contract (reference below).

The Parties will execute a SOW for each set of Buyer Deliverables required. Any ad-hoc Deliverables requirements are to be treated as individual requirements in their own right and the Parties should execute a separate SOW in respect of each, or alternatively agree a Variation to an existing SOW.

All SOWs must fall within the Specification and provisions of the Call-Off Contact.

The details set out within this SOW apply only in relation to the Deliverables detailed herein and will not apply to any other SOWs executed or to be executed under this Call-Off Contract, unless otherwise agreed by the Parties in writing.

Date of SOW: 06 March 2023

SOW Title: Statement of Work 01

SOW Reference:

DOS-WP2114-01

Call-Off Contract Reference: WP21114 GOV.UK Site Search Improvement

Buyer: Cabinet Office

Supplier: Kin and Carta UK Limited

SOW Start Date: 06 March 2023

SOW End Date: 05 December 2023

Duration of SOW: 9 months

Key Personnel (Buyer):

[redacted]

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

[redacted]

[redacted]

Address: The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS

Key Personnel (Supplier):

[redacted]

Address: The Spitfire Building, 71 Collier Street, London, England, N1 9BE. United Kingdom.

1 **Call-Off Contract Specification – Deliverables Context**

SOW Deliverables Background: This Deliverables will focus on deliverables for WP2114 GOV.UK Search Site Improvement

Delivery phase(s): Live

Overview of Requirement: Delivery

2 **Buyer Requirements – SOW**

Deliverables Outcome Description:

Milestone Ref	Milestone Description	Acceptance Criteria	Due Date
MS01	Search vendor evaluation and trial	Selection of best fit search vendor to progress to phase 2 - AB testing using quantitative methodology	week 16 of project
MS02	Implementation of selected search vendor	AB testing conducted with recommendation for production and rollout	week 30 of project
MS03	Suppor and managed t service	Support and handover of the platfor m	week 36 of project

Supplier Resource Plan: Not applicable

Security Applicable to SOW: Not applicable

The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables, have completed Supplier Staff Vetting in accordance with Paragraph 6 (Security of Supplier Staff) of Part B – Annex 1 (Baseline Security Requirements) of Call-Off Schedule 9 (Security).

Cyber Essentials Scheme:

The Buyer requires the Supplier, in accordance with Call-Off Schedule 26 (Cyber Essentials Scheme) to provide a Cyber Essentials Certificate prior to commencing the provision of any Deliverables under this Call-Off Contract.

SOW Standards:

Not applicable.

Performance Management:

A. KPI: Performance to pay process

Met	Partially met	Not met

All of the inputs are submitted in accordance with the performance to pay process timescales and contain accurate and complete information	Inputs are later than prescribed in the performance to pay process but within 5 working days of the prescribed dates • Inputs are incomplete or inaccurate	Inputs are later than 5 working days in the prescribed performance to pay process Inputs contain significant errors

B. KPI: People (resourcing)

Met	**Partially met**	**Not met**
Targets met for all resources or facilities	Targets met for most (50%+) resources or facilities through no fault of the Buyer	Targets missed for most resources or facilities requested through no fault of the Buyer

C. KPI: Partnering behaviours and added value

Met	**Partially met**	**Not met**
● No behavioural problems identified ● Buyer workshops attended and positive contributions made ● Added value recognised by the programme above provision of compensated skilled resource/facilities	● Some minor behavioural problems ● Supplier only attends some workshops or provides minor contributions ● Supplier adds some value above provision of compensated resource and facilities, but this is not regarded as significant	● Significant behavioural problems ● Supplier contributions are rare or insignificant and shows little interest in working with other suppliers ● No added value contributions recognised by the Programme

D.KPI: People in place (Delivery)

Met	**Partially met**	**Not met**

• No resources are swapped out due to deficiency in skill-set and/or no change of facilities is required • No problems identified with quality of work or state of facility • Supplier is making positive team contributions • Supplier skills or facilities meet the standards expected	• Minor issues noted with quality of work or standard of facilities • Few contributions made within team	• Resource is swapped out from project due to deficiency in skill-set or change of facility is required • Persistent issues with quality of work or facilities noted (may be minor ones which have persisted from one month to another) • Significant issue with quality of work or facility noted in a month

The following Material KPIs shall apply to this Call-Off Contract in accordance with Call-Off Schedule 14B (Service Levels and Balanced Scorecard):

Additional Requirements:

Annex 1 – Where Annex 1 of Joint Schedule 11 (Processing Data) in the Call-Off Contract does not accurately reflect the data Processor / Controller arrangements applicable to this Statement of Work, the Parties shall comply with the revised Annex 1 attached to this Statement of Work.

Key Supplier Staff:

Key Role	Key Staff	Contract Details	Employment / Engagement Route (incl. inside/outside IR35)
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[**Indicate**: whether there is any requirement to issue a Status Determination Statement]

SOW Reporting Requirements:

Ref.	**Type of Information**	**Which Services does this requirement apply to?**	**Required regularity of Submission**
1.	Delivery Tracking		
1.2	Delivery tracking - budget burn	All	Weekly

3 Charges

Call Off Contract Charges:

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

- Capped Time and Materials
- Payment of the above Charges will be invoiced at the end of each month on a time and materials basis with NET30 payment terms

The estimated maximum value of this SOW (irrespective of the selected charging method) is £778,350 (excluding VAT and expenses).

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

Reimbursable Expenses:

See Expenses Policy in Call-Off Schedule 5 (Pricing Details and Expenses Policy) and Annex 3 of 'WP2114: Digital Outcomes and Specialists 5 (RM1043.7) Framework Schedule 6: Order Form'.

4 Signatures and Approvals

Agreement of this SOW

BY SIGNING this Statement of Work, the Parties agree that it shall be incorporated into Appendix 1 of the Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:

For and on behalf of the Supplier - Kin and Carta UK Limited

Name: [redacted]

Title: Date: [redacted]

23 February 2023

Signature: DocuSigned by: David Tuck 36213A7392F449B...

For and on behalf of the Buye: Cabinet Office

Name: Title: Date: [redacted]

22nd February 2023

Signature:

Annex 1
Data Processing

Prior to the execution of this Statement of Work, the Parties shall review Annex 1 of Joint Schedule 11 (Processing Data) and if the contents of Annex 1 does not adequately cover the Processor / Controller arrangements covered by this Statement of Work, Annex 1 shall be amended as set out below and the following table shall apply to the Processing activities undertaken under this Statement of Work only:

Data Controller Name: Cabinet Office

Data Processor Name: Kin and Carta UK Limited

Description	**Details**
Identity of Controller for each Category of Personal Data	The Relevant Authority is Controller and the Supplier is Processor The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: ● name and surname; ● a home or work address; ● an email address such as name.surname@company.com; ● Phone number; ● location data;
Duration of the Processing	For the duration of the contract term
Nature and purposes of the Processing	The nature of the Processing is to Identify, test and evaluate a range of managed site search solutions for the GOV.UK website to improve search performance
Type of Personal Data	All Personal Data is as defined with Article 4 (1) of Data Protection Act 2018 (DPA 2018). including:

	name and surname; a home address; an email address such as name.surname@company.com; Phone number; location data;
Categories of Data Subject	Data subject is as defined within the Data Protection Act 2018. • The Authority's Current personnel (including Contractors, Agency Workers and Temporary Workers) • Customers • Suppliers • Application end-users • Website end-users
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	The Supplier shall return all Personal Data to the Buyer upon expiry or End of the Call-Off Contract and shall remove all Personal Data from the Supplier's Property in accordance with Good Industry Practice. Confirmation of deletion of data to be issued to the Buyer as requested.

Annex 3 (Expenses Policy)

Cabinet Office Travel and Expenses Policy:

Annex A - Subsistence rates

UK rates

Overseas

rates

UK rates

UK Lodging rate for rented accommodation
Ceiling - £37 per night.
UK Hotel accommodation rate
Ceiling for bed and breakfast:

London (from centre out to the M25 motorway ring road) - £130.00

Major cities (Aberdeen, Birmingham, Belfast, Bristol, Cardiff, Coventry, Edinburgh, Glasgow, Harlow, Leeds, Liverpool, Manchester, Middlesbrough, Newcastle, Oxford, Portsmouth, Reading, Sheffield, York) - £90.00

Elsewhere - All other locations not mentioned above - £85.

If the cost of breakfast is not included in the accommodation charge a separate payment may be made. The room and breakfast costs overall should remain within the above ceiling. If breakfast cannot be taken because of an early start, a separate breakfast allowance may be paid. See below.
UK Meal allowance
If working more than 5 miles away from your normal place of work you are entitled to claim for:

one meal if away for over 5 hours

two meals if away for 10 to 12 hours

three meals if away for over 12

hours

The ceilings within which you may claim are:

£5 - breakfast

£5 - lunch

£18 - dinner

£23 - combined lunch and dinner

These costs cover food and drink and must be supported by receipts.
The amounts are set at levels which ensure that individuals are not subject to personal tax liabilities, but this is a concession by HMRC and is based on the principle that claims are for subsistence, for example, food and non-alcoholic drinks.

The tax concession could be withdrawn if, for example, staff utilise the allowances for alcoholic drinks instead of the purpose for which they are intended for example, to reimburse out of pocket expenses on food.

Modest expenditure on alcoholic/soft drinks is permissible but if a meal is provided by a third party then a claim solely for alcoholic/soft drinks must not exceed £4 and should be supported by receipts.

Finance will consider claims above the ceiling, only if an individual can provide evidence that purchase within ceilings was impossible and that the higher expenditure was justifiable.

UK Late working meal rate - Actual Expenditure up to a Ceiling of £5

This is a taxable expense and should be claimed via iexpenses using the late/additional attendance template. It is intended to cover periods where a manager makes an unexpected and unscheduled occasional request for an employee to remain working in the office beyond 8pm after completion of a full day's work. .

UK Personal Incidental Hotel Expenses - £5 per night

This payment is flat rate and non-taxable within HM Revenue & Customs (HMRC) limit. It may be claimed to cover out-of-pocket personal expenses (for example laundry, tips, phone calls home) incurred during overnight stays in an hotel or residential training course accommodation. The payment may not be made in conjunction with the flat rate payment for staying with friends or relatives.

UK Staying with friends or relatives rate - £25 per day

This is a flat-rate payment and takes account of all aspects of a 24 hour stay: for example, accommodation, meals, phone calls home and transport between temporary office and place of temporary residence. It may not be claimed in conjunction with the payment for Personal Incidental Expenses.

Following a review of its policy HMRC has withdrawn the tax relief that used to apply to this flat-rate payment and, with effect from April 2009, any claim for a stay with friends or relatives is subject to a tax liability. The Cabinet Office will bear this additional cost. However, in order to ensure that the tax is properly accounted for, you must select the 'Notionally Taxed Expenses' option from the 'Expense Template' drop-down box when creating a claim in RM on Oracle. For those without access to Oracle, there is a similar option on form CO EXP21 in CabWeb.

Overseas rates

Overseas subsistence for hotels, meals and local home to office travel

A separate rate is set for each country to cover meals, accommodation and hotel to office travel. Travel from the airport to hotel will be reimbursed separately. The Expenses Team in finance can advise.

Overseas staying with relatives or friends rate

If you stay with friends or relatives overseas you will receive the residual element of the subsistence allowance payable for the country. It may not be claimed in conjunction with Overseas Personal Incidental Expenses.

A tax liability applies to a stay with relatives and friends overseas, just as it does in the UK It is therefore important that you follow the guidance given above when it comes to submitting a claim for expenses.

Overseas personal incidental hotel expenses

days 1 to 4 = £5 per day

day 5 onwards = £10 per day

This is a flat rate and non-taxable within HMRC limit. It may not be claimed in conjunction with the payment for staying with relatives or friends overseas.

Overseas rented accommodation

This will be determined by the market rate of standard accommodation overseas. Refer to the Overseas Secondment Guide in the Travel Guide for assistance.

Fee paid and non-staff subsistence claims must not exceed the ceilings for permanent employees.

Annex 4

For purposes of GDS' IA Security Schedule herein (Annex 4), this contract is classified as a Standard Consultancy Agreement

1. Definitions

In this Schedule 4 (Security Management):

"Anti-virus Software"	means software that: **(a)** protects the Supplier Information Management System from the possible introduction of Malicious Software; **(b)** scans for and identifies possible Malicious Software in the Supplier Information Management System; **(c)** if Malicious Software is detected in the Supplier Information Management System, so far as possible: **(i)** prevents the harmful effects of the Malicious Software; and **(ii)** removes the Malicious Software from the Supplier Information Management System;
"Breach of Security"	means the occurrence of: **(a)** any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement; **(b)** the loss (physical or otherwise) and/or unauthorised disclosure of any information or data, including copies of such information or data, used

	by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement; and/or **(c)** any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements;
"Buyer Data"	**means any:** (d) 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; or (e) Personal Data for which the Buyer is a, or the, Data Controller, that is: (a) supplied to the Supplier by or on behalf of the Buyer; or (b) that the Supplier generates, processes, stores or transmits under this Agreement.
"Buyer Equipment"	means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;
"Buyer System"	means the information and communications technology system used by the Buyer to interface with the Supplier Information Management System or through which the Buyer receives the Services;
"Certification Default"	**means the occurrence of one or more of the circumstances listed in Paragraph 6.4;**
"Certification Rectification Plan"	**means the plan referred to in Paragraph 6.5.1;**
"Certification Requirements"	**means the information security requirements set out in paragraph 6.**

"Cyber Essentials"	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Plus"	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Scheme"	means the Cyber Essentials scheme operated by the National Cyber Security Centre;
"End-user Device"	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services.
"HMG Baseline Personnel Security Standard"	means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 6.0, May 2018 (https://assets.publishing.service.gov.uk /government/uploads/system/uploads/attachment_data/file/714002/ HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf), as that document is updated from time to time;
'International Data Transfer Agreement	The IDTA and Addendum replaced standard contractual clauses for international transfers. They take into account the binding judgement of the European Court of Justice, in the case commonly referred to as "Schrems II" the IDTA is a transfer tool to comply with Article 46 of the UK GDPR when making restricted transfers
"Malicious Software"	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
"NCSC Cloud Security Principles"	means the National Cyber Security Centre's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www ncsc.gov.uk/collection/cloud-security/ implementing-the-cloud-security-principles.

"NCSC Device Guidance"	means the National Cyber Security Centre's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;
"Privileged User"	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
"Process"	means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data;
"Prohibited Activity"	means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice;
"Prohibition Notice"	means a notice issued under paragraph 1.3 of Annex 1.
"Relevant Certifications"	means those certifications specified in Paragraph 6.1;
"Relevant Convictions"	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), [driving offences, offences against property, drugs, alcohol, public order offences] or any other offences relevant to Services as the Buyer may specify;
"Security Management Plan"	means the document prepared in accordance with the requirements of Paragraph 7
"Sites"	means any premises: **(a)** from or at which:

	(i) the Services are (or are to be) provided; or (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where: (i) any part of the Supplier Information Management System is situated; or (ii) any physical interface with the Buyer System takes place;
"Standard Contractual Clauses"	means the standard data protection clauses specified in Article 46 of the United Kingdom General Data Protection Regulation setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area;
"Supplier Information Management System"	means: (a) those parts of the information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Services; and (b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources);
"Sub-contractor Personnel"	means: (a) any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and (b) engaged in or likely to be engaged in:

	(i) the performance or management of the Services; (ii) or the provision of facilities or services that are necessary for the provision of the Services.
"Supplier Personnel"	means any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor in the management or performance of the Supplier's obligations under this Agreement;
"UKAS"	means the United Kingdom Accreditation Service;

2. Introduction

2.1 This Schedule 4 (Security Management) sets out:

2.1.1 the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of the Buyer Data, the Services and the Supplier Information Management System;

2.1.2 the assessment of this Agreement as either a:

2.1.2.1 Standard consultancy agreement; or

2.1.2.2 Higher-risk consultancy agreement,

in Paragraph 3;

2.1.3 the Buyer's access to the Supplier Personnel and Supplier Information Management System, in Paragraph 4;

2.1.4 the Certification Requirements, in Paragraph 5;

2.1.5 the requirements for a Security Management Plan in the case of higher-risk consultancy agreements, in Paragraph 6;

2.1.6 the security requirements with which the Supplier must comply in Annex 1;

2.1.7 the security requirements applicable to Sub-contractors in Annex 2.

3. Principles of Security

3.1 The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data and, consequently on the security of:

3.1.1 the Sites;

3.1.2 the Services; and

3.1.3 the Supplier's Information Management System.

3.2 Notwithstanding the involvement of the Buyer in the assurance of the Supplier Information Management System, the Supplier remains responsible for:

3.2.1 the security, confidentiality, integrity and availability of the Buyer Data when that Buyer Data is under the control of the Supplier or any of its Sub-contractors; and

3.2.2 the security of the Supplier Information Management System.

3.3 The Supplier shall:

3.3.1 comply with the security requirements in Annex 1; and

3.3.2 ensure that each Sub-contractor that Processes Buyer Data complies with the Sub-contractor security requirements in Annex 2.

3.4 Where the Supplier, a Sub-contractor or any of the Supplier Personnel is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Sub-contractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

4. Buyer Risk Assessment

4.1 The Buyer has assessed this Agreement

as [Buyer to check as appropriate]

□ A standard consultancy agreement;

□ A higher-risk consultancy agreement.

5. Access to Supplier Personnel and Supplier Information Management System

5.1 The Buyer may require, and the Supplier must provide the Buyer and its authorised representatives with:

5.1.1 access to the Supplier Personnel;

5.1.2 access to the Information Management System to audit the Supplier and its Sub-contractors' compliance with this Agreement; and

5.1.3 such other information and/or documentation that the Buyer or its authorised representatives may reasonably require,

to assist the Buyer to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Buyer Data and the Supplier Information Management System are consistent with the representations in the Security Management Plan.

5.2 The Supplier must provide the access required by the Buyer in accordance with Paragraph 5.6 within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within 24 hours of receipt of such request.

6. Certification Requirements

6.1 The Supplier shall ensure that, unless otherwise agreed by the Buyer, it is certified as compliant with:

6.1.1 In the case of a standard consultancy agreement: [Buyer to check as appropriate]

□ Cyber Essentials Plus;

□ Cyber Essentials; or

6.1.2 In the case of a higher-risk consultancy agreement:

6.1.2.1 ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2013; and

6.1.2.2 Cyber Essentials Plus (the "**Relevant Certifications**").

6.2 Unless otherwise agreed by the Buyer, the Supplier must provide the Buyer with a copy of the Relevant Certifications before it begins to provide the Services.

6.3 The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications are:

6.3.1 Currently in effect;

6.3.2 Relate to the full scope of the Supplier Information System; and

6.3.3 Are not subject to any condition that may impact the provision of the Services.

6.4 The Supplier must notify the Buyer promptly, any in any event within three (3) Working Days of becoming aware that:

6.4.1 A Relevant Certification has been revoked or cancelled by the body that awarded it;

6.4.2 A Relevant Certification expired and has not been renewed by the Supplier;

6.4.3 A Relevant Certification no longer applies to the full scope of the Supplier Information Management System or

6.4.4 The body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a "**Certification Default**")

6.5 Where the Supplier has notified the Buyer of a Certification Default under Paragraph 6.4:

6.5.1 the Supplier must, within 10 working Days of the date in which the Supplier provided notice under Paragraph 6.4 (or such other period as the Parties may agree) provide a draft plan (a "**Certification Rectification Plan**") to the Supplier setting out:

6.5.1.1 full details of the Certification Default, including a root cause analysis;

6.5.1.2 the actual and anticipated effects of the Certification Default;

6.5.1.3 the steps the Supplier will take to remedy the Certification Default;

6.5.2 the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

6.5.3 If the Buyer rejects the Certification Rectification Plan, the Buyer must within 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph 3.4.2 will apply to the re-submitted plan;

6.5.4 The rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;

6.5.5 If the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

7. Security Management Plan

Preparation of Security Management Plan

7.1 This Paragraph 6 applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

7.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule 4 (Security Management) and the Agreement in order to ensure the security of the Buyer Data and the Supplier Information Management System.

7.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which must include:

7.3.1 an assessment of the Supplier Information Management System against the requirements of this Schedule 4 (Security Management), including the Annexes;

7.3.2 the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Buyer Data, the Buyer, the Services and/or users of the Services; and

7.3.3 the following information in respect of each Sub-contractor:

7.3.3.1 the Sub-contractor's:

(a) Legal name;

(b) Trading name (if any);

(c) Registration details (where the Sub-contractor is not an individual);

7.3.3.2 the Sites used by the Sub-contractor;

7.3.3.3 the Buyer Data Processed by the Sub-contractor;

7.3.3.4 the Processing that the Sub-contractor will undertake in respect of the Buyer Data;

7.3.3.5 the measures the Sub-contractor has in place to comply with the requirements of this Schedule 4 (Security Management).

7.4 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

7.4.1 an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to Process Buyer Data; or

7.4.2 a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

7.5 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

Updating Security Management Plan

7.6 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.

Monitoring

7.7 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

7.7.1 a significant change to the components or architecture of the Supplier Information Management System;

7.7.2 a new risk to the components or architecture of the Supplier Information Management System;

7.7.3 a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;

7.7.4 a change in the threat profile;

7.7.5 a significant change to any risk component;

7.7.6 a significant change in the quantity of Personal Data held within the Service;

7.7.7 a proposal to change any of the Sites from which any part of the Services are provided; and/or

7.7.8 an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

7.8 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

ANNEX 1: SECURITY REQUIREMENTS

1. Location

1.1 Unless otherwise agreed with the Buyer, the Supplier must, and must ensure that its Sub-contractors must, at all times, store, access or process Buyer Data either:

1.1.1 In the United Kingdom;

1.1.2 The European Economic Area; or

1.1.3 In a facility operated by an entity where:

1.1.3.1 The entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable) containing the Standard Contractual Clauses;

1.1.3.2 The Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the Standard Contractual Clauses;

1.1.3.3 The Supplier has provided the Buyer with such information as the Buyer requires concerning:

(a) The entity;

(b) The arrangements with the entity; and

(c) The entity's compliance with the Standard Contractual Clauses; and

1.1.3.4 The Buyer has not given the Supplier a Prohibition Notice under paragraph 1.3.

1.2 Where the Supplier cannot comply with one or more of the requirements of paragraph 1.1:

1.2.1 it must provide the Buyer with such information as the Buyer requests concerning the security controls in places at the relevant location or locations; and

1.2.2 the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and

1.2.3 if the Buyer does not grant permission to use that location or those locations, the Supplier must cease to store, access or process Buyer Data at that location or those locations within such period as the Buyer may specify.

1.3 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken, the storage, access or Processing Buyer Data as specified in the notice (a "**Prohibited Activity**").

1.3.1 in any particular country or group of countries;

1.3.2 in or using facilities operated by any particular entity or group of entities; or

1.3.3 in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity (a "**Prohibition Notice**").

1.4 Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant Activities affected by the notice, the Supplier must, and must procure that Sub-contractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.

2. Vetting, Training and Staff Access

Vetting before performing or managing Services

2.1 The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel, in any activity relating to the performance and management of the Services unless:

2.1.1 That individual has passed the security checks listed in paragraph 2.2; or

2.1.2 The Buyer has given prior written permission for a named individual to perform a specific role.

2.2 For the purposes of paragraph 2.1, the security checks are:

2.2.1 The checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:

2.2.1.1 The individual's identity;

2.2.1.2 The individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;

2.2.1.3 The individual's previous employment history; and

2.2.1.4 That the individual has no Relevant Convictions;

2.2.2 National security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or

2.2.3 Such other checks for the Supplier Personnel of Sub-contractors as the Buyer may specify.

Annual training

2.3 The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:

2.3.1 General training concerning security and data handling; and

2.3.2 Phishing, including the dangers from ransomware and other malware;

Staff access

2.4 The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.

2.5 The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data,

their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.

2.6 Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel's access to the Buyer Data or part of that Buyer Data specified by the Buyer as soon as practicable and in any event within 24 hours of the request.

Exception for certain Sub-contractors

2.7 Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:

2.7.1 As soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;

2.7.2 Provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Supplier Personnel will perform as the Buyer reasonably requires; and

2.7.3 Comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.

3. Security Testing

3.1 This paragraph applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

Note: the definition of Supplier Information Management System includes those information and communications technology systems that Sub-contractors will use to assist or contribute to the Supplier providing the Services.

3.2 The Supplier must, at the Buyer's option, before providing the Services and when reasonably requested by the Buyer, either:

3.2.1 Conduct security testing of the Supplier Information Management System by:

3.2.1.1 engaging a CHECK Service Provider or a CREST Service Provider;

3.2.1.2 designing and implementing the testing so as to minimise its impact on the Supplier Information Management System and the delivery of the Services; and

3.2.1.3 providing the Buyer with a full, unedited and unredacted copy of the testing report without delay and in any event within 10 Working Days of its receipt by the Supplier; or

3.2.2 Provide details of any security testing undertaken by a CHECK Service Provider or a CREST Service Provider in respect of the Supplier Information Management System in the calendar year immediately preceding the Buyer's request or the Effective Date (as appropriate), including:

3.2.2.1 the parts of the Supplier Information Management System tested;

3.2.2.2 a full, unedited and unredacted copy of the testing report; and

3.2.2.3 the remediation plan prepared by the Supplier to address any vulnerabilities disclosed by the security testing; and

3.2.2.4 the Supplier's progress in implementing that remediation plan.

3.3 The Supplier must remediate any vulnerabilities classified as "medium" or above in the security testing:

3.3.1 before Processing Buyer data where the vulnerability is discovered before the Supplier begins to process Authority Data;

3.3.2 where the vulnerability is discovered when the Supplier has begun to Process Buyer Data:

3.3.2.1 by the date agreed with the Buyer; or

3.3.2.2 where no such agreement is reached:

(a) within 5 Working Days of becoming aware of the vulnerability and its classification where the vulnerability is classified as critical;

(b) within 1 month of becoming aware of the vulnerability and its classification where the vulnerability is classified as high; and

(a) within 3 months of becoming aware of the vulnerability and its classification where the vulnerability is classified as medium.

4. End-user Devices

4.2 The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data is stored or processed in accordance the following requirements:

4.2.1 the operating system and any applications that store, process or have access to Buyer Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

4.2.2 users must authenticate before gaining access;

4.2.3 all Buyer Data must be encrypted using a encryption tool agreed to by the Buyer;

4.2.4 the End-under Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;

4.2.5 the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Buyer Data;

4.2.6 the Suppler or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data on the device and prevent any user or group of users from accessing the device;

4.2.7 all End-user Devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001:2013 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.

4.3 The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.

4.4 Where there any conflict between the requirements of this Schedule 4 (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

5. Encryption

5.1 Unless paragraph 5.2 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer Data is encrypted:

5.1.1 When stored at any time when no operation is being performed on it; and

5.1.2 When transmitted.

5.2 Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 5.1, the Supplier must:

5.2.1 immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

5.2.2 provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;

5.2.3 provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.

5.3 The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.

5.4 This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:

5.4.1 The subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;

5.4.2 The protective measure that the Supplier and/or Sub-contractor will put in please in respect of the unencrypted Buyer Data.

5.5 Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Buyer Data, either party may refer the matter to be determined by an expert in accordance with the Dispute Resolution Procedure..

6. Access Control

6.1 The Supplier must, and must ensure that all Sub-contractors:

6.1.1 identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;

6.1.2 require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;

6.1.3 allow access only to those parts of the Supplier Information Management System and Sites that those persons require;

6.1.4 maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.

6.2 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:

6.2.1 are accessible only from dedicated End-user Devices;

6.2.2 are configured so that those accounts can only be use for system administration tasks;

6.2.3 require passwords with high complexity that are changed regularly;

6.2.4 automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive.

6.3 The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different passwords for their different accounts on the Supplier Information Management System.

6.4 The Supplier must, and must ensure that all Sub-contractors:

6.4.1 configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and

6.4.2 change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

7. Malicious Software

7.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.

7.2 The Supplier shall ensure that such Anti-virus Software:

7.2.1 is configured to perform automatic software and definition updates;

7.2.2 performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and

7.2.3 where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.

7.3 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Buyer Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

7.4 Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 7.3 shall be borne by the parties as follows:

7.4.1 by the Supplier where the Malicious Software originates from the Supplier Software, any third-party software licenced by the Supplier or the Buyer Data (whilst the Buyer Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

7.4.2 by the Buyer, in any other circumstance.

8. Breach of Security

8.1 If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours..

8.2 The Supplier must, upon becoming aware of a Breach of Security or attempted Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other reasonably steps necessary to:

8.2.1 minimise the extent of actual or potential harm caused by such Breach of Security;

8.2.2 remedy such Breach of Security to the extent possible;

8.2.3 apply a tested mitigation against any such Breach of Security; and

8.2.4 prevent a further Breach of Security in the future which exploits the same root cause failure;

8.3 As soon as reasonably practicable and, in any event, within 5 Working Days, or such other period agreed with the Buyer, following the Breach of Security or attempted Breach of Security, provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

8.4 The Supplier must take the steps required by paragraph 8.2 at its own cost and expense.

9. Sub-contractors

9.1 The Supplier must assess the parts of the information and communications technology system and the Sites that its Sub-contractors will use to provide the Services against the NCSC Cloud Security Principles at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Buyer at the Buyer's request.

10. Third-party Software

10.1 The Supplier must not, and must ensure that Sub-contractors do not, use any software to Process Buyer Data where the licence terms of that software purport to grant the licensor

rights to Progress the Buyer Data greater than those rights strictly necessary for the use of the software.

11. Deletion of Buyer Data

11.1 The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor when requested to do so by the Buyer and using a deletion method agreed by the Buyer.