# RM6187 Framework Schedule 6 (Order Form and Call-Off Schedules)

## Order Form

| | |
|---|---|
| CALL-OFF REFERENCE: | project_10882 / ecm_3453 |
| THE BUYER: | Foreign, Commonwealth & Development Office |
| BUYER ADDRESS | King Charles Street London SW1A 2AH |
| THE SUPPLIER: | Deloitte LLP |
| SUPPLIER ADDRESS: | 1 New Street Square, London, EC4A 3HQ |
| REGISTRATION NUMBER: | OC303675 |
| DUNS NUMBER: | 364807771 |
| SID4GOV ID: | n/a |

**Applicable framework contract**
This Order Form is for the provision of the Call-Off Deliverables and dated 27/03/2024. It's issued under the Framework Contract with the reference number RM6187 for the provision of the Lease Management Hub.

**CALL-OFF LOT(S):**
Lot 1

**Call-off incorporated terms**
The following documents are incorporated into this Call-Off Contract.
Where schedules are missing, those schedules are not part of the agreement and can not be used. If the documents conflict, the following order of precedence applies:

1. This Order Form includes the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6187
3. The following Schedules in equal order of precedence:

**Joint Schedules for RM6187 Management Consultancy Framework Three**

- ∉ Joint Schedule 1 (Definitions)
- ∉ Joint Schedule 2 (Variation Form)

- Joint Schedule 3 (Insurance Requirements)
- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

**Call-Off Schedules**

- Call-Off Schedule 9 (Security)

4. CCS Core Terms
5. Joint Schedule 5 (Corporate Social Responsibility)
6. 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**.**

Supplier terms are not 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 start date:** 1st April 2024

**Call-off expiry date:** 30th November 2024

**Call-off initial period:** 8 months

**CALL-OFF OPTIONAL EXTENSION PERIOD**
Not applicable

**Call-off deliverables:**

Operational delivery of a lease management hub to engage overseas Posts, FM Suppliers and Estates, Security & Network Directorate (ESND) to provide such information as is necessary to enable the supplier to process lease events and update the FCDO Integrated Workplace Management Solution (IWMS).

The volume of lease events for processing annually is estimated to be c.2,000 (1,300 Post Hiring Leases, 550 Facilities Management Leases and 150 ESND Leases). The lease events cover new, expiring and modifications to leases including lease term dates, break options, rent reviews, extension options, rental amounts, and calculation of financial and accounting liabilities as either operating or finance leases in accordance with IFRS16 and FCDO's accounting policies.

The lease management hub will;

- Monitor lease event statuses using reports provided by the FCDO Planon development team so the hub has a clear plan of work.
- Engage with Posts, JLL and ESND team in advance of lease events to support timely receipt of information.
- Input lease event data into the FCDO IWMS system (Planon) in line with FCDO process and procedures.
- Conduct quality checking and approvals for lease event data entry into Planon.
- Update Planon to reflect changes in lease liabilities (e.g. rent reviews, stepped rents, indexation events, lease renewals, terminations and expiries) on receipt of instruction to the Hub or notification by Planon.
- Make corrections in Planon that arise from reconciliations within the accounting system as directed by FCDO Finance team in line with FCDO process and procedures.
- Request supporting documentation and evidence from Overseas Posts, FM Provider and ESND and upload documentation to Planon in line with FCDO process and procedures.

The Hub Management team will:

- Provide weekly status updates and management information reporting analytics on the lease management hub performance.
- Provide knowledge transfer and training to the supplier of the long term lease management hub and to transition the service to that long term supplier in accordance with an exit plan.
- Provide access to expertise and knowledge of IFRS16.
- Provide insights through analysis and root cause analysis to suggest process improvements.

All Deloitte team members are UK-based and will operate remotely unless otherwise agreed. Expenses will be incurred in relation to travel, sustenance and accommodation, as required.

## Assumptions and Dependencies

It is the responsibility of the FCDO management team to ensure:

- The scope of work outlined in the Deliverables section is sufficient for FCDO's purpose in relation to IFRS 16.
- The information and data provided to Deloitte is accurate, in all material respects, and is not misleading by omission.
- Deloitte has been advised of all facts and circumstances which could be considered relevant to current leases and any decisions made or likely to be made which would significantly impact FCDO's future leasing strategy.
- Deloitte will retain responsibility for their personnel, including security clearance and day-to-day management and oversight.
- Where required FCDO will provide support with Security Clearance transfers and applications to enable timely onboarding of resource.
- The FCDO team will be clear on timelines and scope of output for the delivery team on specific tasks where necessary. Where there are any changes to timescale and requirements, it is FCDO's responsibility to notify Deloitte of these changes and any supporting policies, processes, etc.
- FCDO retain responsibility for the prioritisation and timely allocation of work for processing, and will communicate this to the Deloitte team as part of weekly governance meetings.
- The FCDO Team will retain responsibility for IT, systems, system security and the provision of data, required to perform this engagement, including access to appropriate Planon functionality.
- The FCDO Team will provide access to the relevant materials, including contracts and associated documentation, systems, documents, policies, procedures, processes, training, and reports to aid Deloitte in delivering the services.
- The FCDO Team sign off on all training materials, process documentation and quality assurance processes.
- The FCDO Team will work the Deloitte team to provide access to relevant stakeholders during the engagement and support any further training or quality checking required to accredit the delivery team.
- The FCDO team will ensure ongoing availability of key FCDO stakeholders to support specific queries/necessary engagement. Technical support may also be required from Planon experts, and/or from subject matter experts in specific areas of Estates or at Post.
- The FCDO team will provide appropriate access (and ongoing support) to IT, data, systems, tools and necessary information in a useable format. Deloitte will not be held accountable for delays in the provision of these services that impact delivery.
- The FCDO Team will retain responsibility for management decisions.
- The Deloitte team will follow established risk and quality frameworks to

perform quality checks on the output of the team. The FCDO is responsible for the timely performance of appropriate quality assurance checking over Deloitte's output (as determined by FCDO).

- FCDO shall retain responsibility for the quality and accuracy of case outcomes and will retain overall accountability to address any subjectivity in application of the review procedures.
- FCDO will inform Deloitte of any relevant controls and sign off requirements in place, to mitigate delivery risk.
- FCDO confirms there is no requirement for an integrated BCDR plan.
- The preparation of financial statements for the FCDO remains the sole responsibility of Management and it is their responsibility to determine the appropriateness of accounting judgements.
- Deloitte will act solely as a Data Processor.
- To provide Posts with a future payments report (FCDO will write the reports in Planon so that they can be run) for Posts to ensure that their payments match and to notify the Hub of any disparities so that they can be resolved in consultation with the Hub.
- To complete Planon data entry and approvals to support FCDO performing the monthly trial closure process and the final monthly close of the IFRS16 accounts.
- To complete Planon data entry and approvals to support FCDO running the annual forecast (on a monthly basis) for each financial year. This will also require the Hub to liaise with ESND, JLL, Posts and Finance to obtain additional lease information which may not be captured in Planon.
- To complete Planon data entry and approval to support the FCDO completing the final year end accounts closure for all IFRS16 liabilities and rights of use to the timetable agreed with Finance.

**Security**
Short form security requirements apply.

All Deloitte staff will be a minimum of SC cleared before beginning work.
Deloitte staff will submit applications for FCDO passes and will follow guidance regarding premise access/ wearing of passes.

**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 (for 8 month period) are: £713,168.00.

**Call-off charges**
As at the Commencement Date, the Buyer is commissioning deliverables as set out

in Call-Off Deliverables and the Price is capped at £713,168.00 (excl. VAT).

Redacted Under FOIA Section 43, Commercial Interests

Charges will be based on Time and Materials and the Supplier will issue an electronic invoice monthly in arrears.

The Supplier will complete timesheets to support the Charges and shall make these available to the Buyer where requested.

The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.

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

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

**Key Performance Indictors (KPI)**

| Topic | Basis of KPI | KPI Evidence |
|---|---|---|
| Accuracy of Service | 95% of events sent for approval to be approved without amendment or rejection. | Data to be contained in Deloitte monthly report |
| | 95% of future lease actions (e.g. rent reviews) to be added to Planon as part of approval process. within 3 working days of receipt of evidence. | Data to be contained in Deloitte monthly report |
| Responsiveness | 80% of lease events to be sent for approval within 3 working days of receipt of evidence. | Data to be contained in Deloitte monthly report |
| | 80% of events sent for approval to be checked within 3 working days | Data to be contained in Deloitte monthly report |
| Management information | Monthly Report format, capturing progress, risks and issues, spend against budget, performance against KPIs, improvements to process etc to be agreed by 26 April 24 | Milestone achieved? |
| | Monthly Report to be received 2 working days in advance of monthly meetings | Milestones achieved? |
| Lessons learnt/Continuous improvement | Workshop to be held with key stakeholders (ESND, JLL and Post) and lessons learned to be | Milestone achieved? |

| | | |
|---|---|---|
| | captured and shared by 31 May 24 | |
| | Introduction of improvements to process and delivery to be evidenced. Examples could include but are not limited to: proactive chasing of lease actions, use of standard FCDO lease template where possible etc | Lessons learned log to be maintained that provides evidence of improvements made |
| Training and Development | Training organised with all relevant stakeholders (ESND, JLL, Post) that should include lessons learned, regular errors that arise etc | Milestone achieved?<br><br>Feedback captured from stakeholders at the end of training events or through short questionnaires. |
| | Effective training and handover to the incoming service provider | Feedback from new service provider regarding how well planned and how well delivered the handover process was. |
| Budget Monitoring | Regular review of resourcing requirements and spend to meet demand with a view to finding efficiencies and potentially driving savings. | Regular review of spend against budget |

**Reimbursable expenses**

Recoverable as stated in Framework Schedule 3 (Framework Prices) paragraph 4.

**Payment method**

Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

The Buyer will provide the Supplier with a Purchase Order number. Supplier will invoice the Buyer for services used under the contract and send these to: UKPCInvoices@fcdo.gov.uk

**Key Performance Indictors (KPI)**

**Buyer's invoice address**

Redacted Under FOIA Section 40, Personal Information

Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information

**FINANCIAL TRANSPARENCY OBJECTIVES**

Not applicable

**Buyer's authorised representative**
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information

**Buyer's security policy**
Available on request

**Supplier's authorised representative**
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information

**Supplier's contract manager**
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information

**Progress report frequency**
Weekly

**Progress meeting frequency**
Weekly, every Thursday

**Key staff**

Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information

Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information

Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information
Redacted Under FOIA Section 40, Personal Information

**Key subcontractor(s)**
Not applicable

**Commercially sensitive information**

- Supplier's rate card

**Service credits**

Not applicable

**Additional insurances**

Not applicable

**Guarantee**

Not applicable

**Buyer's environmental and social value policy**

n/a

**Social value commitment**

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender)]

**Formation of call off contract**

By signing and returning this Call-Off Order Form the Supplier agrees to enter a Call-Off Contract with the Buyer to provide the Services in accordance with the Call-Off Order Form and the Call-Off Terms.

The Parties hereby acknowledge and agree that they have read the Call-Off Order Form and the Call-Off Terms and by signing below agree to be bound by this Call-Off Contract.

**For and on behalf of the Supplier**:

[to be signed via Docusign]

**For and on behalf of the Buyer**:

[to be signed via Docusign]

# 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:

i. the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

ii. the Call-Off Contract Effective Date in respect of the Additional Insurances.

2.1 The Insurances shall be:

i. maintained in accordance with Good Industry Practice;

ii. (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

iii. taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

iv. maintained for at least six (6) years after the End Date.

3.1 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

## 2. How to manage the insurance

4.1 Without limiting the other provisions of this Contract, the Supplier shall:

i. 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;

ii. promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

iii. Hold all policies in respect of the Insurances and cause any insurance broker affecting 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

5.1 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.

6.1 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

7.1 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

8.1 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

9.1 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.

10.1 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

## 7. Insurance claims

11.1 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 cooperate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

12.1 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.

13.1 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

14.1 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 five million pounds (£5,000,000);

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

3.1 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).

# Joint Schedule 4 (Commercially Sensitive Information)

**1. What is 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.

2.1 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).

3.1 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 | 20/03/2024 | Call Off Schedule 4: Call Off Tender. | 7 years |
| 2 | 20/03/2024 | Schedule 6: Order Form | 7 years |

# Joint Schedule 11 (Processing Data)

## Definitions

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

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

## Status of the Controller

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

(1) "Controller" in respect of the other Party who is "Processor";
(2) "Processor" in respect of the other Party who is "Controller";
(3) "Joint Controller" with the other Party;
**(4)** "Independent Controller" of the Personal Data where the other Party is also "Controller",

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

## Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.
4. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

(1) a systematic description of the envisaged Processing and the purpose of the Processing;
(2) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
(3) an assessment of the risks to the rights and freedoms of Data Subjects; and
(4) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

(1) Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
(2) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may

reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

1. nature of the data to be protected;
2. harm that might result from a Personal Data Breach;
3. state of technological development; and
4. cost of implementing any measures;

(3) ensure that :

1. the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));
2. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

a. are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;
b. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
c. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
d. have undergone adequate training in the use, care, protection and handling of Personal Data;

(4) not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

1. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
2. the Data Subject has enforceable rights and effective legal remedies;
3. the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
4. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

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

7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

(1) receives a Data Subject Access Request (or purported Data Subject Access Request);
(2) receives a request to rectify, block or erase any Personal Data;
(3) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
(4) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
(5) 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
(6) becomes aware of a Personal Data Breach.

8. The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
9. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

(1) the Controller with full details and copies of the complaint, communication or request;
(2) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
(3) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
(4) assistance as requested by the Controller following any Personal Data Breach; and/or
(5) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(1) the Controller determines that the Processing is not occasional;
(2) 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
(3) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
13. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

(1) notify the Controller in writing of the intended Subprocessor and Processing;
(2) obtain the written consent of the Controller;
(3) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
(4) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

14. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).
16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

**Where the Parties are Joint Controllers of Personal Data**

17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

**Independent Controllers of Personal Data**

18. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
19. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
22. The Parties shall only provide Personal Data to each other:

(1) to the extent necessary to perform their respective obligations under the Contract;

(2) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

*(3)* where it has recorded it in Annex 1 *(Processing Personal Data).*

23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

(1) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

(2) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

1. promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
2. provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

26. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

(1) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

(2) implement any measures necessary to restore the security of any compromised Personal Data;

(3) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

(4) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

*27.* Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

28. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 28 of this Joint Schedule 11.

**Annex 1 - Processing Personal Data**

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

1.1.1.1 The contact details of the Relevant Authority's Data Protection Officer are: Redacted Under FOIA Section 40, Personal Information

2.1.1.1 The contact details of the Supplier's Data Protection Officer are: Redacted Under FOIA Section 40, Personal Information

3.1.1.1 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

4.1.1.1 Any such further instructions shall be incorporated into this Annex.

| Description | Details |
|---|---|
| Identity of Controller for each Category of Personal Data | **The Relevant Authority is Controller and the Supplier is Processor**<br><br>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: |

| | |
|---|---|
| | Estates and/or lease agreement data: including access to names, addresses, and landlord bank account details.<br><br>**The Parties are Independent Controllers of Personal Data**<br><br>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:<br>Business contact details of Supplier Personnel for which the Supplier is the Controller,<br>Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller |
| Duration of the Processing | *1st April 2024 – 30th November 2024* |
| Nature and purposes of the Processing | The processing of lease data enables FCDO to track it's leasehold assets, pay landlords, comply with International Financial Accounting Standard (IFRS) 16, and to meet it's obligations to accommodate staff safely overseas and in the UK. |
| Type of Personal Data | Name, address, telephone number, of primary property occupant, number of adults and children in occupation, landlord's name, contact details, and bank account. |
| Categories of Data Subject | Staff (including volunteers, agents, and temporary workers) |
| Plan for return and destruction of the data once the Processing is complete<br><br>UNLESS requirement under Union or Member State law to preserve that type of data | Data to be processed on FCDO systems. |

# 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:<br>any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or<br>the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,<br>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 has been updated from time to time. |

**2. Complying with security requirements and updates to them**

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

2.1 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.

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

4.1 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.

5.1 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**

1.1 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.

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

i. is in accordance with the Law and this Contract;
ii. as a minimum demonstrates Good Industry Practice;
iii. meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and
iv. where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.

3.1 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.

4.1 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**

**1.1 Introduction**

i. 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.

**2.1 Content of the Security Management Plan**

i. The Security Management Plan shall:

1. comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;
2. identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
3. 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;
4. 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;
5. 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;

6. 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
7. 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.

**3.1 Development of the Security Management Plan**

i. 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.

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

iii. 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.

iv. 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.

**4.1 Amendment of the Security Management Plan**

i. The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:
   1. emerging changes in Good Industry Practice;
   2. any change or proposed change to the Deliverables and/or associated processes;
   3. where necessary in accordance with paragraph 2.2, any change to the Security Policy;
   4. any new perceived or changed security threats; and
   5. any reasonable change in requirements requested by the Buyer.

ii. 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:
   1. suggested improvements to the effectiveness of the Security Management Plan;
   2. updates to the risk assessments; and

3. suggested improvements in measuring the effectiveness of controls.

iii. 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.

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

**5. Security breach**

1.1 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.

2.1 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:

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

1. minimise the extent of actual or potential harm caused by any Breach of Security;
2. 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;
3. prevent an equivalent breach in the future exploiting the same cause failure; and
4. 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.

3.1 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.