



## RM6100 Technology Services 3 Agreement

### Framework Schedule 4 - Annex 1

#### Lots 2, 3 and 5 Order Form

## Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 with a start date of 16 June 2021 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms. The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website. The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

The Supplier shall provide the Services and/or Goods specified in this Order Form (including any attachments to this Order Form) to the Buyer on and subject to the terms of the Contract for the duration of the Contract Period.



In this Order Form, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) of the Call-Off Terms

This Order Form shall comprise:

1. This document headed “Order Form”;
2. Attachment 1 – Services Specification;
3. Attachment 1A – CQ Log
4. Attachment 1B - Contract negotiations
5. Attachment 2 – Charges and Invoicing;
6. Attachment 3 – Implementation Plan;
7. Attachment 4 – Service Levels and Service Credits;
8. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
9. Attachment 6 – Software;
10. Attachment 7 – Financial Distress;
11. Attachment 8 - Governance
12. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
13. Attachment 10 – ServiceNow flow ups; and
14. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.



The Order of Precedence shall be as set out in Clause 2.2 of the Call-Off Terms being:

- 1.1.1 the Framework, except Framework Schedule 18 (Tender);
- 1.1.2 the Order Form;
- 1.1.3 the Call Off Terms; and
- 1.1.4 Framework Schedule 18 (Tender).

Within the Order Form, Attachment 10 (ServiceNow flow ups) shall take precedence over the rest of the Order Form for elements of the Services that are provided by the ServiceNow vendor. The Buyer consents to ServiceNow UK Limited ("**ServiceNow**") being a Sub-processor for the purposes of Clause 34.12.



## Section A

### General information

Contract Details	
Contract Reference:	CCTS22A85
Contract Title:	Provision of a Civil Service Employee Transfer Platform
Contract Description:	The digital Civil Service employee transfer service will enable all civil servants to move from one department to another, at pace and without friction. The service will be used by all Civil Service organisations including arm's length bodies (ALB's) and non-departmental public bodies (NDPBs).
Contract Anticipated Potential Value:	The maximum contract value including any extension options is £6,300,000.00. Extensions are subject to additional approval.



this should set out the total potential value of the Contract	
---	--

<b>Estimated Year 1 Charges:</b>	TBC on award.
----------------------------------	---------------

<b>Commencement Date:</b>	27/03/2023
---------------------------	------------

<b>Buyer details</b>
<b>Buyer organisation name</b>
Cabinet Office



**Billing address**

Redacted Text Under FOIA Section 40, Personal Information

**Buyer representative name**

The name of your point of contact for this Order

Redacted Text Under FOIA Section 40, Personal Information

**Buyer representative contact details**

Email and telephone contact details for the Buyer's representative. This must include an email for the purpose of Clause 50.6 of the Contract.

Redacted Text Under FOIA Section 40, Personal Information

**Buyer Project Reference**

Please provide the customer project reference number.

Redacted Text Under FOIA Section 40, Personal Information



#### Supplier details

##### Supplier name

Fujitsu Services Limited

##### Supplier registered address

Lovelace Road, Bracknell, England, RG12 8SN

##### Supplier representative name

Redacted Text Under FOIA Section 40, Personal Information

##### Supplier representative contact details

Email and telephone contact details of the supplier's representative. This must include an email for the purpose of Clause 50.6 of the Contract.

Redacted Text Under FOIA Section 40, Personal Information



**Order reference number or the Supplier's Catalogue Service Offer Reference Number**

Procurement Reference: CCTS22A85

## Section B

### Part A – Framework Lot

**Framework Lot under which this Order is being placed**

*Tick one box below as applicable (unless a cross-Lot Further Competition or Direct Award, in which case, tick Lot 1 also where the buyer is procuring technology strategy & Services Design in addition to Lots 2, 3 and/or 5. Where Lot 1 is also selected then this Order Form and corresponding Call-Off Terms shall apply and the Buyer is not required to complete the Lot 1 Order Form.*

1. TECHNOLOGY STRATEGY & SERVICES DESIGN	<input type="checkbox"/>
2. TRANSITION & TRANSFORMATION	<input type="checkbox"/>





3. OPERATIONAL SERVICES	
a: End User Services	<input type="checkbox"/>
b: Operational Management	<input type="checkbox"/>
c: Technical Management	<input type="checkbox"/>
d: Application and Data Management	X
5. SERVICE INTEGRATION AND MANAGEMENT	<input type="checkbox"/>



## Part B – The Services Requirement

### Commencement Date

See above in Section A

### Contract Period

*Guidance Note – this should be a period which does not exceed the maximum durations specified per Lot below:*

Lot	Maximum Term (including Initial Term and Extension Period) – Months (Years)
2	36 (3)



3	60 (5)
5	60 (5)

**Initial Term** Months

48 months

**Extension Period (Optional)** Months

12 months, 60 Days' notice of any extension to be given before expiry

**Minimum Notice Period for exercise of Termination Without Cause**

(Calendar days) Insert right (see Clause 35.1.9 of the Call-Off Terms): 30 (Thirty)

**Sites for the provision of the Services**

*Guidance Note - Insert details of the sites at which the Supplier will provide the Services, which shall include details of the Buyer Premises, Supplier premises and any third party premises.*

The Supplier shall provide the Services from the following Sites:

**Buyer Premises:**



Not Applicable

**Supplier Premises:**

Not Applicable

**Third Party Premises:**

Not Applicable

**Buyer Assets**

*Guidance Note: see definition of Buyer Assets in Schedule 1 of the Call-Off Terms*

Not Applicable



### Additional Standards

*Guidance Note: see Clause 13 (Standards) and the definition of Standards in Schedule 1 of the Contract. Schedule 1 (Definitions). Specify any particular standards that should apply to the Contract over and above the Standards.*

Not Applicable

### Buyer Security Policy

*Guidance Note: where the Supplier is required to comply with the Buyer's Security Policy then append to this Order Form below.*

Supplier to complete Annex B - IA Supplier Questionnaire

### Buyer ICT Policy

*Guidance Note: where the Supplier is required to comply with the Buyer's ICT Policy then append to this Order Form below.*

Not Applicable



## Insurance

*Guidance Note: if the Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Agreement or the Buyer requires any additional insurances please specify the details below.*

Third Party Public Liability Insurance (£) - Not Applicable

Professional Indemnity Insurance (£) - Not Applicable

Covered under the framework agreement. No additions required.

## Buyer Responsibilities

*Guidance Note: list any applicable Buyer Responsibilities below.*

Buyer Responsibilities are the Cabinet Office responsibilities set out in the attached document:

Redacted Text Under FOIA Section 43, Commercial Interests



## Goods

*Guidance Note: list any Goods and their prices.*

Not Applicable

## Governance – Option Part A or Part B

*Guidance Note: the Call-Off Terms has two options in respect of governance. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is limited project governance required during the Contract Period.*

Governance Schedule	Tick as applicable
Part A – Short Form Governance Schedule	<input checked="" type="checkbox"/>
Part B – Long Form Governance Schedule	<input type="checkbox"/>

The Part selected above shall apply this Contract.



### Change Control Procedure – Option Part A or Part B

*Guidance Note: the Call-Off Terms has two options in respect of change control. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is no requirement to include a complex change control procedure where operational and fast track changes will not be required.*

Change Control Schedule	Tick as applicable
Part A – Short Form Change Control Schedule	<input type="checkbox"/>
Part B – Long Form Change Control Schedule	<input checked="" type="checkbox"/>

The Part selected above shall apply this Contract. Where Part B is selected, the following information shall be incorporated into Part B of Schedule 5 (Change Control Procedure):

- for the purpose of Paragraph 3.1.2 (a), the figure shall be £ [TBC on contract commencement];  
and
- for the purpose of Paragraph 8.2.2, the figure shall be £ [TBC on contract commencement].





## Section C

### Part A - Additional and Alternative Buyer Terms

#### **Additional Schedules and Clauses** (see Annex 3 of Framework Schedule 4)

*This Annex can be found on the RM6100 CCS webpage. The document is titled RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5.*

#### **Part A – Additional Schedules**

*Guidance Note: Tick any applicable boxes below*

<b>Additional Schedules</b>	<b>Tick as applicable</b>
S1: Implementation Plan	<input type="checkbox"/>
S2: Testing Procedures	<input type="checkbox"/>
S3: Security Requirements (either Part A or Part B)	Part A <input checked="" type="checkbox"/> or Part B <input type="checkbox"/>
S4: Staff Transfer - see Part B below which states that Part E only of Additional Schedule S4 (Staff Transfer) will apply	<input type="checkbox"/>



S5: Benchmarking	<input type="checkbox"/>
S6: Business Continuity and Disaster Recovery	X
S7: Continuous Improvement	<input type="checkbox"/>
S8: Guarantee	<input type="checkbox"/>
S9: MOD Terms	<input type="checkbox"/>

#### Part B – Additional Clauses

*Guidance Note: Tick any applicable boxes below*

Additional Clauses	Tick as applicable
C1: Relevant Convictions	<input type="checkbox"/>
C2: Security Measures	<input type="checkbox"/>
C3: Collaboration Agreement	<input type="checkbox"/>



Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

### Part C - Alternative Clauses

*Guidance Note: Tick any applicable boxes below*

The following Alternative Clauses will apply:

Alternative Clauses	Tick as applicable
Scots Law	<input type="checkbox"/>
Northern Ireland Law	<input type="checkbox"/>
Joint Controller Clauses	<input type="checkbox"/>

Where selected above the Alternative Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.



## Part B - Additional Information Required for Additional Schedules/Clauses Selected in Part A

### Additional Schedule S3 (Security Requirements)

*Guidance Note: where Schedule S3 (Security Requirements) has been selected in Part A of Section C above, then for the purpose of the definition of "Security Management Plan" insert the Supplier's draft security management plan below.*

To be provided on contract commencement

### Additional Schedule S4 (Staff Transfer)

*Guidance Note: where Schedule S4 (Staff Transfer) has been selected in Part A of Section C above, then for the purpose of the definition of "Fund" in Annex D2 (LGPS) of Part D (Pension) insert details of the applicable fund below.*

Part E of Additional Schedule S4 (Staff Transfer) will apply for the purposes of this call-off contract

### Additional Clause C1 (Relevant Convictions)



*Guidance Note: where Clause C1 (Relevant Convictions) has been selected in Part A of Section C above, then for the purpose of the definition of "Relevant Convictions" insert any relevant convictions which shall apply to this contract below.*

Not Applicable

#### **Additional Clause C3 (Collaboration Agreement)**

*Guidance Note: where Clause C3 (Collaboration Agreement) has been selected in Part A of Section C above, include details of organisation(s) required to collaborate immediately below.*

Not Applicable



## Section D

### Supplier Response

#### Commercially Sensitive information

Any confidential information that the Supplier considers sensitive for the duration of an awarded Contract should be included here. Please refer to the definition of Commercially Sensitive Information in the Contract – *use specific references to sections rather than copying the relevant information here.*

Redacted Text Under FOIA Section 43, Commercial Interests

## Section E

### Contract Award



This Call Off Contract is awarded in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100.

**SIGNATURES**

**For and on behalf of the Supplier**

Name	
Job role/title	
Signature	
Date	

**For and on behalf of the Buyer**

Name	
Job role/title	
Signature	
Date	



Crown  
Commercial  
Service

## **Attachment 1 – Services Specification**

### **Part A – Statement of Requirements**

**Redacted Text Under FOIA Section 43, Commercial Interests**





## **Part B (Outline Service Descriptions)**

Redacted Text Under FOIA Section 43, Commercial Interests

## **Part C (Supplementary Provisions relating to the Statement of Requirements)**

1. Section 6 of the Statement of Requirements in Part A of Attachment 1 states that the Supplier will meet the requirements listed in Annex A - Specification of Requirements. It is hereby agreed that the Supplier will not be required to meet the following requirements in Annex A:

Redacted Text Under FOIA Section 43, Commercial Interests

2. It is acknowledged that certain of the provisions of the Statement of Requirements are superseded by the other Attachments in this Contract such as Attachment 2 (Charges and Invoicing) regarding Milestones and Schedule 6 (Service Levels) regarding Service Levels.



Crown  
Commercial  
Service

## Attachment 1A CQ Log

**Redacted Text Under FOIA Section 43, Commercial Interests**



Crown  
Commercial  
Service

## Attachment 1B Contract Negotiation Correspondence

Redacted Text Under FOIA Section 43, Commercial Interests



## **Attachment 2 – Charges and Invoicing**

### **Part A – Milestone Payments and Delay Payments**

**Redacted Text Under FOIA Section 43, Commercial Interests**

### **Part B – Service Charges**

**Redacted Text Under FOIA Section 43, Commercial Interests**

### **Part C – Supplier Personnel Rate Card for Calculation of Time and Materials Charges**

**Redacted Text Under FOIA Section 43, Commercial Interests**



Crown  
Commercial  
Service

## **Part D – Risk Register**

Not applicable.

## **Part E - Early Termination (as per clause 36.2)**

**Redacted Text Under FOIA Section 43, Commercial Interests**



Crown  
Commercial  
Service

## Attachment 3 – Outline Implementation Plan

Redacted Text Under FOIA Section 43, Commercial Interests



## Attachment 4 – Service Levels and Service Credits

### Service Levels and Service Credits

#### Redacted Text Under FOIA Section 43, Commercial Interests

##### Critical Service Level Failure

In the event of poor performance, defined as the failure to meet the contractual target for the KPIs, the Cabinet Office shall meet with the Supplier to understand and determine the root causes of the issue. When required, the Supplier must formulate a performance improvement plan to rectify the issues. Cabinet Office will monitor the outcomes of the performance plan to evidence improvements have been made and the required performance levels met.

This performance improvement plan must be actioned and performed to demonstrably meet satisfactory levels of performance within 30 days of the start date of the plan being executed. Where the Supplier fails to deliver the plan to the required standard and the supplier continues to fail to meet contractual KPIs, the Cabinet Office reserves the right to terminate the contract.

## Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

- 1.1.5 The Parties agree that they will update this Attachment 5 periodically to record any changes to Key Supplier Personnel and/or any Key Sub-Contractors appointed by the Supplier after the Commencement Date for the purposes of the delivery of the Services.



## Part A – Key Supplier Personnel

Key Supplier Personnel	Key Role(s)	Duration
TBC on Contract Commencement	TBC on Contract Commencement	TBC on Contract Commencement

## Part B – Key Sub-Contractors

Key Sub-contractor name and address (if not the same as the registered office)	Registered office and company number	Related product/Service description	Key Sub-contract price expressed as a percentage of total projected Charges over the Contract Period	Key role in delivery of the Services
N/A	N/A	N/A	N/A	N/A





## Attachment 6 – Software

- 1.1.1 The Software below is licensed to the Buyer in accordance with Clauses 20 (*Intellectual Property Rights*) and 21 (*Licences Granted by the Supplier*) – except for ServiceNow where the terms in Attachment 10 (ServiceNow Flow Ups) shall apply.
- 1.1.2 The Parties agree that they will update this Attachment 6 periodically to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

### Part A – Supplier Software

The Supplier Software includes the following items:

Software	Supplier (if an Affiliate of the Supplier)	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/ Expiry
N/A							

### Part B – Third Party Software



The Third Party Software shall include the following items:

Third Party Software	Supplier	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/ Expiry
ServiceNow	ServiceNow UK Limited	HR/ITSM/Platform	Up to 24,000 HR users per annum.  No technical limitation. Acquiring licences above 24,000 is subject to change control processes.	See Attachment 10	N/A	COTS	Term

## Attachment 7 – Financial Distress

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the following shall apply:

### PART A – CREDIT RATING THRESHOLD

Entity	Credit Rating (long term) <i>(insert credit rating issued for the entity at the Commencement Date)</i>	Credit Rating Threshold <i>(insert the actual rating (e.g. AA-) or the Credit Rating Level (e.g. Credit Rating Level 3))</i>
<b>Supplier</b>	[Rating Agency 1] – [insert rating for Rating Agency 1]	[Rating Agency 1] – [insert threshold for Rating Agency 1]
	[Rating Agency 2] – [insert rating for Rating Agency 2]	[Rating Agency 2] – [insert threshold for Rating Agency 2]
	[etc.]	[etc.]
<b>[Guarantor]</b>	[Rating Agency 1] – [insert rating for Rating Agency 1]	[Rating Agency 1] – [insert threshold for Rating Agency 1]
	[Rating Agency 2] – [insert rating for Rating Agency 2]	[Rating Agency 2] – [insert threshold for Rating Agency 2]
	[etc.]	[etc.]
<b>[Key Sub-contractor 1]</b>	[etc.]	[etc.]
<b>[Key Sub-contractor 2]</b>	[etc.]	[etc.]

### PART B – RATING AGENCIES

[Rating Agency 1 (e.g Standard and Poors)]

- Credit Rating Level 1 = [AAA]
- Credit Rating Level 2 = [AA+]

- Credit Rating Level 3 = [AA]
- Credit Rating Level 4 = [AA-]
- Credit Rating Level 5 = [A+]
- Credit Rating Level 6 = [A]
- Credit Rating Level 7 = [A-]
- Credit Rating Level 8 = [BBB+]
- Credit Rating Level 9 = [BBB]
- Credit Rating Level 10 = [BBB-]
- Etc.

- [Rating Agency 2 (e.g Moodys) ]
- Credit Rating Level 1 = [Aaa]
- Credit Rating Level 2 = [Aa1]
- Credit Rating Level 3 = [Aa2]
- Credit Rating Level 4 = [Aa3]
- Credit Rating Level 5 = [A1]
- Credit Rating Level 6 = [A2]
- Credit Rating Level 7 = [A3]
- Credit Rating Level 8 = [Baa1]
- Credit Rating Level 9 = [Baa2]
- Credit Rating Level 10 = [Baa3]
- Etc.
- [Rating Agency 3 (etc.) ]
- Credit Rating Level 1 = [XXX]
- Etc.

# Attachment 8 – Governance

## PART A – SHORT FORM GOVERNANCE

For the purpose of Part A of Schedule 7 (Short Form Governance) of the Call-Off Terms, the following board shall apply:

Operational Board	
Buyer Members for the Operational Board	TBA on contract commencement
Supplier Members for the Operational Board	TBA on contract commencement
Frequency of the Operational Board	TBA on contract commencement
Location of the Operational Board	TBA on contract commencement

## Attachment 9 – Schedule of Processing, Personal Data and Data Subjects

This Attachment 9 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 Schedule shall be with the Buyer at its absolute discretion.

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

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

1.1.1.3 The Processor shall comply with any further written instructions with respect to processing by the Controller.

1.1.1.4 Any such further instructions shall be incorporated into this Attachment 9.

Description	Details
Identity of Controller for each Category of Personal Data	Redacted Text Under FOIA Section 43, Commercial Interest
Duration of the processing	Redacted Text Under FOIA Section 43, Commercial Interest
Nature and purposes of the processing	Redacted Text Under FOIA Section 43, Commercial Interest
Type of Personal Data	Redacted Text Under FOIA Section 43, Commercial Interest

Categories of Data Subject	Redacted Text Under FOIA Section 43, Commercial Interest
<p>Plan for return and destruction of the data once the processing is complete</p> <p>UNLESS requirement under union or member state law to preserve that type of data</p>	Redacted Text Under FOIA Section 43, Commercial Interest

## Attachment 10 – ServiceNow Flow Ups

Redacted Text Under FOIA Section 43, Commercial Interest

### Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses

#### S3 SECURITY REQUIREMENTS

##### PART A – SHORT FORM SECURITY REQUIREMENTS

#### 1. DEFINITIONS

- 1.1 In this Part A of Schedule S3 (Security Requirements), the following definitions shall apply:

<b>"Security Management Plan"</b>	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 is set out in the Order Form and as updated from time to time.
-----------------------------------	--

#### 2. COMPLIANCE WITH SECURITY REQUIREMENTS AND UPDATES

- 2.1 The Supplier shall comply with the Security Policy and the requirements of this Schedule S3 (Security Requirements) including the Security Management Plan (if any) and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.
- 2.2 Where the Security Policy applies, the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.
- 2.3 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 Services it may propose a Change 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 then be subject to the Change Control Procedure.
- 2.4 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Change Control Procedure the Supplier shall continue to provide the Services in accordance with its existing obligations.

#### 3. SECURITY STANDARDS

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



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

- 3.2.1 is in accordance with the Law and this Contract;
- 3.2.2 as a minimum demonstrates Good Industry Practice;
- 3.2.3 meets any specific security threats of immediate relevance to the Services and/or the Buyer Data; and
- 3.2.4 where specified by the Buyer in accordance with Paragraph The Supplier shall comply with the Security Policy and the requirements of this Schedule S3 (Security Requirements) including the Security Management Plan (if any) and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy. complies with the Security Policy and the ICT Policy.

#### 1.1

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

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

## 4. SECURITY MANAGEMENT PLAN

### Introduction

4.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Part A of Schedule S3 (Security Requirements). The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

### Content of Security Management Plan

4.2 The Security Management Plan shall:

- 4.2.1 comply with the principles of security set out in Paragraph SECURITY STANDARDS and any other provisions of this Contract relevant to security;
- 4.2.2 identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
- 4.2.3 detail the process for managing any security risks from Sub-Contractors and third parties authorised by the Buyer with access to the Services, processes associated with the provision of the Services, the Buyer Premises, the Sites and any IT, information and data (including the Buyer's Confidential Information and the Buyer Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;

- 4.2.4 be developed to protect all aspects of the Services and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any IT, information and data (including the Buyer's Confidential Information and the Buyer 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 Services;
- 4.2.5 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services 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 Services comply with the provisions of this Contract;
- 4.2.6 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 The Supplier shall comply with the Security Policy and the requirements of this Schedule S3 (Security Requirements) including the Security Management Plan (if any) and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy. the Security Policy; and
- 4.2.7 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 Services and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Part A Schedule S3 (Security Requirements).

#### **Development of the Security Management Plan**

- 4.3 Within twenty (20) Working Days after the Commencement Date and in accordance with Paragraph SECURITY MANAGEMENT PLAN, 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 set out in the Order Form.
- 4.4 If the Security Management Plan submitted to the Buyer in accordance with Paragraph Within twenty (20) Working Days after the Commencement Date and in accordance with Paragraph 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 set out in the Order Form., or any subsequent revision to it in accordance with Paragraph SECURITY MANAGEMENT PLAN, 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 Part A Schedule S3 (Security Requirements). If the Security Management Plan is not approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.
- 4.5 The Buyer shall not unreasonably withhold or delay its decision to approve or not the Security Management Plan pursuant to Paragraph If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3, or any subsequent revision to it in accordance with Paragraph 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 Part A Schedule S3 (Security Requirements). 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.. 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 The Security Management Plan shall: shall be deemed to be reasonable.

- 4.6 Approval by the Buyer of the Security Management Plan pursuant to Paragraph If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3, or any subsequent revision to it in accordance with Paragraph 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 Part A Schedule S3 (Security Requirements). 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. or of any change to the Security Management Plan in accordance with Paragraph SECURITY MANAGEMENT PLAN shall not relieve the Supplier of its obligations under this Part A Schedule S3 (Security Requirements).

#### **Amendment of the Security Management Plan**

- 4.7 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:
- 4.7.1 emerging changes in Good Industry Practice;
  - 4.7.2 any change or proposed change to the Services and/or associated processes;
  - 4.7.3 where necessary in accordance with Paragraph The Supplier shall comply with the Security Policy and the requirements of this Schedule S3 (Security Requirements) including the Security Management Plan (if any) and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy., any change to the Security Policy;
  - 4.7.4 any new perceived or changed security threats; and
  - 4.7.5 any reasonable change in requirements requested by the Buyer.
- 4.8 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:
- 4.8.1 suggested improvements to the effectiveness of the Security Management Plan;

4.8.2 updates to the risk assessments; and

4.8.3 suggested improvements in measuring the effectiveness of controls.

4.9 Subject to Paragraph 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 Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment., 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 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:, a request by the Buyer or otherwise) shall be subject to the Change Control Procedure.

4.10 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 Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment.

## **5. SECURITY BREACH**

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

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

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

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

5.3.2 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;

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

5.3.4 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.

5.4 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 The Supplier shall comply with the

Security Policy and the requirements of this Schedule S3 (Security Requirements) including the Security Management Plan (if any) and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.) or the requirements of this Part A Schedule S3 (Security Requirements), then any required change to the Security Management Plan shall be at no cost to the Buyer.

## S6 BUSINESS CONTINUITY AND DISASTER RECOVERY

### Definitions

1.1 In this Schedule, the following definitions shall apply:

<b>BCDR Plan"</b>	has the meaning given to it in Paragraph At least ninety (90) Working Days prior to the Commencement Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a "BCDR Plan"), which shall detail the processes and arrangements that the Supplier shall follow to: of this Schedule;
<b>Business Continuity Plan"</b>	has the meaning given to it in Paragraph Section 2 which shall relate to business continuity (the "Business Continuity Plan"); and of this Schedule;
<b>Disaster Recovery Plan"</b>	has the meaning given to it in Paragraph Section 3 which shall relate to disaster recovery (the "Disaster Recovery Plan"). of this Schedule;
<b>Related Supplier"</b>	any person who provides services to the Buyer which are related to the Services from time to time;
<b>Review Report"</b>	has the meaning given to it in Paragraph the Supplier's proposals (the "Supplier's Proposals") for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan. of this Schedule; and
<b>Supplier's Proposals"</b>	has the meaning given to it in Paragraph the Supplier's proposals (the "Supplier's Proposals") for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan. of this Schedule;

## 2. BCDR Plan

- 2.1 Within ninety (90) Working Days prior to the Commencement Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a "**BCDR Plan**"), which shall detail the processes and arrangements that the Supplier shall follow to:
- 2.1.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Services; and
  - 2.1.2 the recovery of the Services in the event of a Disaster
- 2.2 The BCDR Plan shall be divided into three sections:
- 2.2.1 Section 1 which shall set out general principles applicable to the BCDR Plan;
  - 2.2.2 Section 2 which shall relate to business continuity (the "**Business Continuity Plan**"); and
  - 2.2.3 Section 3 which shall relate to disaster recovery (the "**Disaster Recovery Plan**").
- 2.3 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

## 3. General Principles of the BCDR Plan (Section 1)

- 3.1 Section 1 of the BCDR Plan shall:
- 3.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;
  - 3.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Services and any goods and/or services provided to the Buyer by a Related Supplier;
  - 3.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;
  - 3.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;
  - 3.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;
  - 3.1.6 contain a risk analysis, including:
    - (a) failure or disruption scenarios and assessments of likely frequency of occurrence;
    - (b) identification of any single points of failure within the provision of the Services and processes for managing those risks;
    - (c) identification of risks arising from the interaction of the provision of the Services with the goods and/or services provided by a Related Supplier; and
    - (d) a business impact analysis of different anticipated failures or disruptions;

3.1.7 provide for documentation of processes, including business processes, and procedures;

3.1.8 set out key contact details for the Supplier (and any Sub-Contractors) and for the Buyer;

3.1.9 identify the procedures for reverting to "normal service";

3.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;

3.1.11 identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and

3.1.12 provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans.

3.2 The BCDR Plan shall be designed so as to ensure that:

3.2.1 the Services are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;

3.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;

3.2.3 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and

3.2.4 it details a process for the management of disaster recovery testing.

3.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Services and the business operations supported by the provision of Services.

3.4 The Supplier shall not be entitled to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

#### **4. Business Continuity (Section 2)**

4.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Services remain supported and to ensure continuity of the business operations supported by the Services including:

4.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of the Services; and

4.1.2 the steps to be taken by the Supplier upon resumption of the provision of the Services in order to address the effect of the failure or disruption.

4.2 The Business Continuity Plan shall:

4.2.1 address the various possible levels of failures of or disruptions to the provision of Services;

4.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Services; and

4.2.3 set out the circumstances in which the Business Continuity Plan is invoked.

## **5. Disaster Recovery (Section 3)**

- 5.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
- 5.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:
  - 5.2.1 loss of access to the Buyer Premises;
  - 5.2.2 loss of utilities to the Buyer Premises;
  - 5.2.3 loss of the Supplier's helpdesk or CAFM system;
  - 5.2.4 loss of a Sub-Contractor;
  - 5.2.5 emergency notification and escalation process;
  - 5.2.6 contact lists;
  - 5.2.7 staff training and awareness;
  - 5.2.8 BCDR Plan testing;
  - 5.2.9 post implementation review process;
  - 5.2.10 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;
  - 5.2.11 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and
  - 5.2.12 testing and management arrangements.

## **6. Review and changing the BCDR Plan**

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



- 6.2 Each review of the BCDR Plan pursuant to Paragraph The Supplier shall review the BCDR Plan: shall assess its suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.
- 6.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.
- 6.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
- 6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Services.

## **7. Testing the BCDR Plan**

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

7.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

7.5.3 the Supplier's proposals for remedying any such failures.

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

## **8. Invoking the BCDR Plan**

- 8.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.