

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

Order Form

CALL-OFF REFERENCE: **C3911**

THE BUYER: The Comptroller-General of patents, designs, and trade marks, acting through the Patent Office and operating in the name of the Intellectual Property Office.

BUYER ADDRESS REDACTED

THE SUPPLIER: Reward Gateway (UK) Ltd

SUPPLIER ADDRESS: REDACTED

REGISTRATION NUMBER: REDACTED

DUNS NUMBER: REDACTED

APPLICABLE FRAMEWORK CONTRACT:

CCS RM6273 Employee Benefits and Services (Lot 1: Managed Service)

This Order Form is for the provision of the Call-Off Deliverables and dated 18 August 2025. It's issued under the Framework Contract with the reference number RM6273 Employee Benefits and Services for the provision of Employee Benefits & Services to IPO.

CALL-OFF LOT(S):
Lot 1 – Managed Services

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing, we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6273 Employee Benefits and Services framework reference number]
3. Framework Special Terms (To be advised if applicable)
4. The following Schedules in equal order of precedence (To be reviewed at contract award):

- **Joint Schedules for RM6273 Employee Benefits and Services**

- Joint Schedule 2 (Variation Form)
- Joint Schedule 3 (Insurance Requirements)
- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 7 (Financial Difficulties)
- Joint Schedule 9 (Minimum Standards of Reliability)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

- **Call-Off Schedules for RM6273 Employee Benefits and Services**

- Call-Off Schedule 1 (Transparency Reports)
- Call-Off Schedule 3 (Continuous Improvement)
- Call-Off Schedule 5 (Pricing Details)
- Call-Off Schedule 6 (ICT Services)
- Call-Off Schedule 7 (Key Supplier Staff)
- Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
- Call-Off Schedule 9 (Security)
- Call-Off Schedule 10 (Exit Management)
- Call-Off Schedule 13 (Implementation Plan and Testing)
- Call-Off Schedule 14 (Service Levels)
- Call-Off Schedule 15 (Call-Off Contract Management)
- Call-Off Schedule 18 (Background Checks)
- Call-Off Schedule 20 (Call-Off Specification)

CCS Core Terms (version 3.0.11)

5. Joint Schedule 5 (Corporate Social Responsibility) **RM6273 Employee Benefits and Services**
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.

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

CALL-OFF SPECIAL TERMS

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

Should the Deliverables under the Call-Off Contract include any of the following Services:

- a) Financial Wellbeing;
- b) Green Cars
- c) Payroll Giving; or
- d) Cycle to work,

as these Services constitute regulated financial activities or have other regulatory requirements, the Buyer will be required to sign an agreement directly with the Supplier's Subcontractor, being the provider of those Services, in addition to the Call-Off Contract, in a form to be agreed between the Buyer and the Subcontractor.

CALL-OFF START DATE: 1st November 2025

CALL-OFF EXPIRY DATE: 31st October 2029

CALL-OFF INITIAL PERIOD: 4 Years (with break clause at 15 months*)

* The Comptroller-General of patents, designs, and trade marks, acting through the Patent Office and operating in the name of the Intellectual Property Office. ('the Buyer') reserves the right to exercise a 'break clause' after the initial 15 months of the contract (by 1 February 2027).

This will permit the Buyer to terminate the contract after the first anniversary of the commencement date by giving written notice of termination of at least 60 days, to the desired termination date. Reward Gateway (UK) Ltd would have transition obligations upon termination as outlined in Section 6.6 of the Specification (Call-Off Schedule 20).

EXTENSIONS AVAILABLE:

Subject to internal Buyer approval and budget availability there is the option to extend the contract by two (2) separate periods of twelve (12) months. The sanctioning of the extension options is entirely at the Buyer's discretion.

CALL-OFF DELIVERABLES

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

MAXIMUM LIABILITY

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

The Estimated Year 1 Charges used to calculate liability in the first Contract Year are: £ REDACTED

CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES

Recoverable as stated in the Framework Contract

PAYMENT METHOD

BACS

BUYER'S INVOICE ADDRESS:

Payment will only be made on satisfactory delivery of the agreed services and functionality. Before payment, any invoices that are received must include a detailed breakdown of the work completed, the associated costs and quote a reference number.

All invoices must quote a relevant IPO Purchase Order and Contract reference number and be emailed to REDACTED.

Payment will be made within 30 days of receipt of invoice.

Please note: Reward Gateway (UK) Ltd shall notify the IPO immediately and in advance if the organisational account is to be put on hold and provide the reasons for this. Reward Gateway (UK) Ltd must provide sufficient notice to the IPO to enable the IPO to resolve the issue and minimise disruption for orders being processed.

BUYER'S AUTHORISED REPRESENTATIVE

REDACTED,
REDACTED

BUYER'S ENVIRONMENTAL POLICY

[Our energy use - Intellectual Property Office - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

BUYER'S SECURITY POLICY

See Annex A (Below)

SUPPLIER'S AUTHORISED REPRESENTATIVE

REDACTED, REDACTED

SUPPLIER'S CONTRACT MANAGER

REDACTED, REDACTED
REDACTED, REDACTED

PROGRESS REPORT FREQUENCY

REDACATED

PROGRESS MEETING FREQUENCY

REDACTED

KEY STAFF

REDACTED, REDACTED
REDACTED, REDACTED

KEY SUBCONTRACTOR(S)

Not Applicable

COMMERCIALLY SENSITIVE INFORMATION

- Technical Question responses (Call-Off Schedule 4 (Call-Off Tender))
- Pricing (Call-Off Schedule 5 (Pricing Details))

SERVICE CREDITS

REDACTE

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

REDACTED

Reward Gateway (UK) Ltd Representative:

Signed by an authorised signatory for and behalf of the Supplier

Supplier_Signature

REDACTED, REDACTED

REDACTED, REDACTED

14th October 2025

For and on behalf of the Buyer

Contracting_Authority_Signature

REDACTED, REDACTED

REDACTED, REDACTED

14th October 2025

Annex A – IPO Security Policy



Security Policy for Contractors / Consultants / Suppliers

1. This document specifies the requirements that must be met by contractors in the handling, management, storage and processing of information belonging to the IPO or its partners.

Information Security

2. Information security is the preservation of confidentiality, integrity and availability of IPO information. Information risk means the risks to the security of IPO's information.

Objectives

3. IPO requires the security of its information to be maintained in order to ensure that the IPO is able to rely on its information for its business needs and meets its statutory, regulatory and HM Government policy obligations.
4. IPO maintains an Information Security Management System and applies security controls consistent with ISO 27001:2013.

Information Risk Assessment and Management

5. IPO employs risk assessment methodologies consistent with HMG guidance ([NCSC Risk Management Introduction](#)) and ISO 27005:2018.
6. Residual information risks can only be accepted by the IPO Executive Board through the Chief Security Officer.

Incident Breach Reporting

7. IPO requires that any breach or incident involving IPO assets, information, personnel or that has an adverse effect to the IPO, be reported as soon as practicable to REDACTED

Legislative, Regulatory and Contractual Requirements

8. The management of IPO and other official information may engage obligations under the following legislation (note that this list is not exhaustive):

- The Official Secrets Act 1911 to 1989;
- Public Records Act 1958 and 1967;
- The Health and Safety Act 1976 (and as amended by Health and Safety (Offences) Act 2008);
- Police and Criminal Evidence Act 1984;
- Copyright Designs and Patents Act 1988;
- Patents Act 1977;
- Patents Rules 2007 & the Patents (Fees) Rules 2007;
- Trade Marks Act 1938 and 1994;
- Trade Marks Rules 2008
- Trade Marks (International Registration) Order 2008
- Registered Designs Act & Rules
- Civil Evidence Act 1968 and 1995;
- Criminal Procedure and Investigations Act 1996;
- Human Rights Act 1998;
- Data Protection Act 2018;
- UK General Data Protection Regulation 2021
- Civil Contingencies Act 2004;
- Electronic Communications Act 2000, and as amended by Statutory Instrument 2003 No. 2426 (The Privacy and Electronic Communications (EC Directive) Regulations 2003);
- Freedom of Information Act 2000;
- Regulation of Investigatory Powers Act 2000 as amended by Statutory Instrument 2000 No. 2699 (Lawful Business Regulations);
- Criminal Justice Act 2003;

- Computer Misuse Act 1990; and as amended by Police and Justice Act 2006.
 - Proceeds of Crime Act 2002
 - Public Contracts Regulations 2015
 - Company Names Adjudicator Rules 2008
 - Enterprise Act 2016
9. IPO is required to comply with HM Government policy on information security and assurance including:
- Government Functional Standard GovS 007: Security
 - The Government Security Classification Policy
10. Any organisation accessing, processing, communicating or managing IPO information must do so such that IPO's legal, policy and regulatory obligations are met.
11. Any transfer of IPO information to a third-party must be authorised, via the IPO Information Asset Transfer Request process. Processing of personal data outside of the UK or European Economic Area (EEA), is not permissible without the agreement of the IPO Data Protection Manager. All transferring arrangements must be supported by an agreed legal documentation such as MoU, Data Sharing Agreement or contract between IPO and Data Processors.
12. Anyone accessing official IPO information, including through provision of goods or services to IPO will be bound by the terms of the Official Secrets Act 1989.

Access to IPO Information, Information Assets and Information Systems

13. Anyone required to access IPO information and/or work in an IPO building must either hold or be prepared to apply for a Baseline Personnel Security Standard (BPSS) clearance. This entails identity, nationality and criminal record checks. BPSS clearances obtained through other government departments may be accepted by IPO. If access is required to information at higher levels of security classification, additional national security vetting checks may be required. If access to specific IT systems or Administrator access is required, Security Clearance or Enhanced Security Clearance may be required. This clearance must be in place prior to commencement of access.
14. Access to information assets and systems will be the minimum necessary to achieve business purposes.

15. When the need to access IPO information, assets and systems ends, all IPO equipment (e.g. laptops, security passes, etc) must be returned to IPO prior to the termination of a contract.
16. IPO may monitor the use of its information, information assets and information systems for lawful business purposes.
17. Anyone granted access to IPO technical systems must comply with the requirements of IPO Secure Handbook including its Acceptable Use Policy. Failure to comply with these policies and other relevant instructions may constitute a breach of contract and lead to termination or legal action.
18. Removable media (including laptops) may only be used to manage IPO information with the explicit consent of the IPO Secure team. Any removable media must be encrypted to a degree commensurate with the security classification of the information held within the removable media as required by HMG standards.
19. Supplier personnel may only enter IPO premises with an appropriate security pass issued by the IPO and may only enter areas of IPO premises commensurate with their function and, where appropriate (for example, in security areas), escorted by IPO staff.

Information Security Management System Controls

20. Where a supplier is contracted to manage IPO information, information assets or information systems, the supplier must ensure that an information security management system employed to secure IPO information, information assets or information systems is in place and preferably complies with ISO/IEC 27001:2013. Cyber Security Essentials will be considered as a minimum. Where ISO/IEC 27001:2013 or Cyber Security Essentials is not held, a decision will be made by the IPO Chief Security Officer. Evidence must be provided to IPO of compliance with the standard, either through formal certification or otherwise to IPO Secure's satisfaction before any IPO information, information assets or information systems are accessed by the supplier.
21. Suppliers must agree to permit and facilitate audits of all aspects of their information security management system by IPO and to address any findings of such audits in order to preserve the security of information to IPO's standards and requirements.
22. The transmission of information between IPO and a supplier must be encrypted to a level commensurate with the security classification of the information and to HMG standards.
23. Live IPO data and information may not be used for test purposes.

24. IPO information may not be copied by any supplier other than as far as is necessary for providing an agreed service to IPO.
25. Suppliers must have a security incident reporting process in place to a standard and design acceptable to IPO to ensure that any incidents involving IPO information are immediately reported to IPO Secure via REDACTED. Suppliers must agree to undertake any remedial action required by the IPO and ensure that this is implemented in an auditable way.
26. A supplier holding IPO data on IPO's behalf must have in place processes to ensure that critical IPO information held by them can be promptly and efficiently recovered following an emergency.
27. All IPO information held in support of an agreement with a third-party must be destroyed or returned to the IPO at the end of the agreement. The IPO will determine, which approach is appropriate when setting out the working arrangements.

JOINT SCHEDULES:

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contract Details

Joint Schedule 2 (Variation Form)

Crown Copyright 2018

This variation is between:	The Comptroller-General of patents, designs, and trade marks, acting through the Patent Office and operating in the name of the Intellectual Property Office. ("the Buyer") And Reward Gateway (UK) Ltd ("the Supplier")	
Contract name:	[insert name of contract to be changed] ("the Contract")	
Contract reference number:	[insert contract reference number]	
Details of Proposed Variation		
Variation initiated by:	[delete as applicable: Buyer/Supplier]	
Variation number:	[insert variation number]	
Date variation is raised:	[insert date]	
Proposed variation		
Reason for the variation:	[insert reason]	
An Impact Assessment shall be provided within:	[insert number] days	
Impact of Variation		
Likely impact of the proposed variation:	[Supplier to insert assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: <ul style="list-style-type: none"> [Buyer to insert original Clauses or Paragraphs to be varied and the changed clause] 	
Financial variation:	Original Contract Value:	£ [insert amount]
	Additional cost due to variation:	£ [insert amount]
	New Contract value:	£ [insert amount]

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by the Buyer
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Joint Schedule 2 (Variation Form)

Crown Copyright 2018

Signed by an authorised signatory for and on behalf of the Buyer

Signature

Date

Name (in Capitals)

Address

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature

Date

Name (in Capitals)

Address

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need to have

- 1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:
 - 1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
 - 1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.
- 1.2 The Insurances shall be:
 - 1.2.1 maintained in accordance with Good Industry Practice;
 - 1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;
 - 1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
 - 1.2.4 maintained for at least six (6) years after the End Date.
- 1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. How to manage the insurance

- 2.1 Without limiting the other provisions of this Contract, the Supplier shall:
 - 2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;
 - 2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
 - 2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other

evidence of placing cover representing any of the Insurances to which it is a party.

3. What happens if you aren't insured

- 3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.
- 3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. Evidence of insurance you must provide

- 4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. Making sure you are insured to the required amount

- 5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. Cancelled Insurance

- 6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
- 6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

- 7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in

dealing with such claims including without limitation providing information and documentation in a timely manner.

- 7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.
- 7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

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

professional indemnity insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than] one million pounds (£1,000,000);

public liability insurance [with cover (for a single event or a series of related events and in the aggregate)] of not less than one million pounds (£1,000,000); and

employers' liability insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than] ten million pounds (£10,000,000).

Joint Schedule 4 (Commercially Sensitive Information)

REDACTED

Joint Schedule 6 (Key Subcontractors)

1. Restrictions on certain subcontractors

- 1.1 The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.
- 1.2 The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.
- 1.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to section 18 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:
 - 1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
 - 1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
 - 1.3.3 the proposed Key Subcontractor employs unfit persons.
- 1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:
 - 1.4.1 the proposed Key Subcontractor's name, registered office and company registration number;
 - 1.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;
 - 1.4.3 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm's-length" terms;
 - 1.4.4 for CCS, the Key Sub-Contract price expressed as a percentage of the total projected Framework Price over the Framework Contract Period;
 - 1.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and
 - 1.4.6 (where applicable) Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.

Joint Schedule 6 (Key Subcontractors)

Crown Copyright 2018

- 1.5 If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:
 - 1.5.1 a copy of the proposed Key Sub-Contract; and
 - 1.5.2 any further information reasonably requested by CCS and/or the Buyer.
- 1.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:
 - 1.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;
 - 1.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;
 - 1.6.3 a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;
 - 1.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;
 - 1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:
 - (a) the data protection requirements set out in Clause 14 (Data protection);
 - (b) the FOIA and other access request requirements set out in Clause 16 (When you can share information);
 - (c) the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;
 - (d) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and
 - (e) the conduct of audits set out in Clause 6 (Record keeping and reporting);
 - 1.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the Buyer can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and
 - 1.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

Joint Schedule 7 (Financial Difficulties)

Definitions

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

"Credit Rating Threshold"	1 the minimum credit rating level for the Monitored Company as set out in Annex 2 and
"Financial Distress Event"	2 the occurrence or one or more of the following events: <ul style="list-style-type: none">a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold;b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects;c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party;d) Monitored Company committing a material breach of covenant to its lenders;e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; orf) any of the following:<ul style="list-style-type: none">i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract;ii) non-payment by the Monitored Company of any financial indebtedness;

	<p>iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or</p> <p>iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company</p> <p>3 in each case which CCS reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Call-Off Contract;</p>
"Financial Distress Service Continuity Plan"	4 a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with [each Call-Off] Contract in the event that a Financial Distress Event occurs;
"Monitored Company"	5 Supplier [the Guarantor] or any Key Subcontractor]
"Rating Agencies"	6 the rating agencies listed in Annex 1.

When this Schedule applies

The Parties shall comply with the provisions of this Schedule in relation to the assessment of the financial standing of the Monitored Companies and the consequences of a change to that financial standing.

The terms of this Schedule shall survive:

under the Framework Contract until the later of (a) the termination or expiry of the Framework Contract or (b) the latest date of termination or expiry of any call-off contract entered into under the Framework Contract (which might be after the date of termination or expiry of the Framework Contract); and

under the Call-Off Contract until the termination or expiry of the Call-Off Contract.

What happens when your credit rating changes

The Supplier warrants and represents to CCS that as at the Start Date the long term credit ratings issued for the Monitored Companies by each of the Rating Agencies are as set out in Annex 2.

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

If there is any downgrade credit rating issued by any Rating Agency for the Monitored Company the Supplier shall ensure that the Monitored Company's

auditors thereafter provide CCS within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by CCS (such requests not to exceed 4 in any Contract Year) with written calculations of the quick ratio is not currently used] the quick ratio for the Monitored Company as at the end of each Contract Year or such other date as may be requested by CCS. For these purposes the "quick ratio" on any date means:

$$\frac{A + B + C}{D}$$

where:

A	is the value at the relevant date of all cash in hand and at the bank of the Monitored Company];
B	is the value of all marketable securities held by the Supplier the Monitored Company determined using closing prices on the Working Day preceding the relevant date;
C	is the value at the relevant date of all account receivables of the Monitored]; and
D	is the value at the relevant date of the current liabilities of the Monitored Company].

The Supplier shall:

regularly monitor the credit ratings of each Monitored Company with the Rating Agencies; and

promptly notify (or shall procure that its auditors promptly notify) CCS in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

For the purposes of determining whether a Financial Distress Event has occurred the credit rating of the Monitored Company shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated the Monitored Company at or below the applicable Credit Rating Threshold.

What happens if there is a financial distress event

In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if CCS becomes aware of the Financial Distress Event without notification and brings the event to the attention of the

Supplier), the Supplier shall have the obligations and CCS shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

In the event that a Financial Distress Event arises due to a Key Subcontractor notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute then, CCS shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:

rectify such late or non-payment; or

demonstrate to CCS's reasonable satisfaction that there is a valid reason for late or non-payment.]

The Supplier shall and shall procure that the other Monitored Companies shall:

at the request of CCS meet CCS as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) to review the effect of the Financial Distress Event on the continued performance of each Contract and delivery of the Deliverables in accordance each Call-Off Contract; and

where CCS reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1) that the Financial Distress Event could impact on the continued performance of each Contract and delivery of the Deliverables in accordance with each Call-Off Contract:

submit to CCS for its Approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within ten (10) Working Days of the initial notification (or awareness) of the Financial Distress Event); and

provide such financial information relating to the Monitored Company as CCS may reasonably require.

If CCS does not (acting reasonably) approve the draft Financial Distress Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to CCS within five (5) Working Days of the rejection of the first or subsequent (as the case may be) drafts. This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by CCS or referred to the Dispute Resolution Procedure.

If CCS considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not remedy the relevant Financial Distress Event, then it may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the Dispute Resolution Procedure.

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

- on a regular basis (which shall not be less than Monthly), review the Financial Distress Service Continuity Plan and assess whether it remains adequate and up to date to ensure the continued performance each Contract and delivery of the Deliverables in accordance with each Call-Off Contract;

- where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1, submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 4.5 and 4.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and

- comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).

Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.

CCS shall be able to share any information it receives from the Buyer in accordance with this Paragraph with any Buyer who has entered into a Call-Off Contract with the Supplier.

When CCS or the Buyer can terminate for financial distress

CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:

- the Supplier fails to notify CCS of a Financial Distress Event in accordance with Paragraph 3.4;

- CCS and the Supplier fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 4.3 to 4.5; and/or

- the Supplier fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraph 4.6.3.

If the Contract is terminated in accordance with Paragraph 5.1, Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply as if the Contract had been terminated under Clause 10.4.1.

What happens If your credit rating is still good

Without prejudice to the Supplier's obligations and CCS' and the Buyer's rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:

the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and

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

ANNEX 1: RATING AGENCIES

Dun & Bradstreet

ANNEX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

Entity	Credit rating (long term)
Supplier	40
Guarantor	40
Key Subcontractor	40

Joint Schedule 9 (Minimum Standards of Reliability)

1. Standards

1.1 No Call-Off Contract with an anticipated contract value in excess of £20 million (excluding VAT) shall be awarded to the Supplier if it does not show that it meets the minimum standards of reliability as set out in the OJEU Notice (“**Minimum Standards of Reliability**”) at the time of the proposed award of that Call-Off Contract.

1.2 CCS shall assess the Supplier’s compliance with the Minimum Standards of Reliability:

1.2.1 upon the request of any Buyer; or

1.2.2 whenever it considers (in its absolute discretion) that it is appropriate to do so.

1.3 In the event that the Supplier does not demonstrate that it meets the Minimum Standards of Reliability in an assessment carried out pursuant to Paragraph 1.2, CCS shall so notify the Supplier (and any Buyer in writing) and the CCS reserves the right to terminate its Framework Contract for material Default under Clause 10.4 (When CCS or the Buyer can end this contract).

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan		
Details of the Default:		
Deadline for receiving the [Revised] Rectification Plan:	[add date (minimum 10 days from request)]	
Signed by [Buyer] :		Date:
Supplier [Revised] Rectification Plan		
Cause of the Default	[add cause]	
Anticipated impact assessment:	[add impact]	
Actual effect of Default:	[add effect]	
Steps to be taken to rectification:	Steps	Timescale
	1.	[date]
	2.	[date]
	3.	[date]
	4.	[date]
	[...]	[date]
Timescale for complete Rectification of Default	[X] Working Days	
Steps taken to prevent recurrence of Default	Steps	Timescale
	1.	[date]
	2.	[date]
	3.	[date]

Joint Schedule 10 (Rectification Plan)

Crown Copyright 2018

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

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:

- (a) “Controller” in respect of the other Party who is “Processor”;
- (b) “Processor” in respect of the other Party who is “Controller”;
- (c) “Joint Controller” with the other Party;
- (d) “Independent Controller” of the Personal Data where the other Party is also “Controller”,

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

Where one Party is Controller and the other Party its Processor

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:

- (a) a systematic description of the envisaged Processing and the purpose of the Processing;
 - (b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
- (a) Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
 - (b) ensure that it has in place Protective Measures, 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:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Personal Data Breach;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
 - (c) ensure that :
 - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) 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;
 - (d) 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:
 - (i) 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;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
 - (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
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:
- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
 - (b) receives a request to rectify, block or erase any Personal Data;
 - (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
 - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - (f) becomes aware of a Personal Data Breach.
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:
 - (a) the Controller with full details and copies of the complaint, communication or request;
 - (b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (d) assistance as requested by the Controller following any Personal Data Breach; and/or
 - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
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:
 - (a) the Controller determines that the Processing is not occasional;
 - (b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
 - (c) 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:
 - (a) notify the Controller in writing of the intended Subprocessor and Processing;
 - (b) obtain the written consent of the Controller;
 - (c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

- (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
- 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:
 - (a) to the extent necessary to perform their respective obligations under the Contract;

- (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
 - (c) 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”**):
 - (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
- 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:

- (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
 - (b) implement any measures necessary to restore the security of any compromised Personal Data;
 - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
 - (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
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 The contact details of the Relevant Authority's Data Protection Officer are: REDACTED
- 1.2 The contact details of the Supplier's Data Protection Officer is Peter Lewinton Data Protection & Compliance Officer REDACTED.
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	The Parties are Independent Controllers of Personal Data The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation.
Duration of the Processing	From the outset of the Framework Agreement date, and up to 6 years after the expiry or termination of the Framework Agreement in order to meet legal obligations.
Nature and purposes of the Processing	Any operation carried out for the purposes of processing applications under the Order Form
Type of Personal Data	Full name Workplace address Workplace Phone Number Workplace email address
Categories of Data Subject	Customer Staff Authority Staff Workers

<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>	<p>The personal data will be retained for each data subject for up to 6 years after the expiry or termination of the Framework Agreement.</p>
--	---

Annex 2 - Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 18-28 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

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

- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
- (b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- (c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
- (d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and
- (e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Relevant Authority each undertake that they shall:

- (a) report to the other Party every [x] months on:

- (i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
- (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
- (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
- (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
- (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

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

- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
- (e) request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

- (g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
 - (i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;
 - (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
 - (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
- (h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Personal Data Breach;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
- (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and
- (j) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

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

3. Data Protection Breach

- 3.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming

aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and
- (b) all reasonable assistance, including:
 - (i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
 - (ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
 - (iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
 - (iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

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

- (a) the nature of the Personal Data Breach;
- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Personal Data Breach; and

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

4. **Audit**

4.1 The Supplier shall permit:

- (a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or
- (b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. **Impact Assessments**

5.1 The Parties shall:

- (a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and
- (b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. **ICO Guidance**

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

7. Liabilities for Data Protection Breach

- 7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:
- (a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;
 - (b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or
 - (c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).
- 7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.
- 7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

- (a) if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;
- (b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
- (c) if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

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

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

9. Sub-Processing

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

- (a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
- (b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

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

taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

CALL-OFF SCHEDULES

Call-Off Schedule 1 (Transparency Reports)

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

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
[Performance]	[]	[]	[]
[Call-Off Contract Charges]	[]	[]	[]
[Key Subcontractors]	[]	[]	[]
[Technical]	[]	[]	[]
[Performance management]	[]	[]	[]

Call-Off Schedule 3 (Continuous Improvement)

Buyer's Rights

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

Supplier's Obligations

The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.

The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.

In addition to Paragraph 2.1, the Supplier shall produce at the start of each Contract Year a plan for improving the provision of Deliverables and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year ("**Continuous Improvement Plan**") for the Buyer's Approval. The Continuous Improvement Plan must include, as a minimum, proposals:

identifying the emergence of relevant new and evolving technologies;

changes in business processes of the Supplier or the Buyer and ways of working that would provide cost savings and/or enhanced benefits to the Buyer (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);

new or potential improvements to the provision of the Deliverables including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Deliverables; and

measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives.

The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred (100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.

The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.

The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.

If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.

Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:

the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and

the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.

The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.

All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.

Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.

At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.

Call-Off Schedule 4 (Call Off Tender): Reward Gateway / Edenred

REDACTED

Call-Off Schedule 5 (Pricing Details)

REDACTED

Call-Off Schedule 6 (ICT Services)

1. Definitions

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

"Buyer Property"	the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract;
"Buyer Software"	any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;
"Buyer System"	the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
"Commercial off the shelf Software" or "COTS Software"	Non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms
"Defect"	any of the following: <ul style="list-style-type: none">a) any error, damage or defect in the manufacturing of a Deliverable; orb) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; orc) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

- d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;

"Emergency Maintenance"

ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;

"ICT Environment"

the Buyer System and the Supplier System;

"Licensed Software"

all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;

"Maintenance Schedule"

has the meaning given to it in paragraph 8 of this Schedule;

"Malicious Software"

any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;

"New Release"

an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;

"Open Source Software"

computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use,

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

	study, change and distribute the software to any and all persons and for any and all purposes free of charge;
"Operating Environment"	<p>means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which:</p> <p>the Deliverables are (or are to be) provided; or</p> <p>the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or</p> <p>where any part of the Supplier System is situated;</p>
"Permitted Maintenance"	has the meaning given to it in paragraph 8.2 of this Schedule;
"Quality Plans"	has the meaning given to it in paragraph 6.1 of this Schedule;
"Sites"	has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;
"Software"	Specially Written Software COTS Software and non-COTS Supplier and third party Software;
"Software Supporting Materials"	has the meaning given to it in paragraph 9.1 of this Schedule;
"Source Code"	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
"Specially Written Software"	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;

"Supplier System"

the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

- 2.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT Services which are part of the Deliverables.

3. Buyer due diligence requirements

- 3.1. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;
- 3.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;
 - 3.1.2. operating processes and procedures and the working methods of the Buyer;
 - 3.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and
 - 3.1.4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.
- 3.2. The Supplier confirms that it has advised the Buyer in writing of:
- 3.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;
 - 3.2.2. the actions needed to remedy each such unsuitable aspect; and
 - 3.2.3. a timetable for and the costs of those actions.

4. Licensed software warranty

- 4.1. The Supplier represents and warrants that:
 - 4.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the Buyer which are necessary for the performance of the Supplier's obligations under this Contract including the receipt of the Deliverables by the Buyer;
 - 4.1.2. all components of the Specially Written Software shall:
 - 4.1.2.1. be free from material design and programming errors;
 - 4.1.2.2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels) and Documentation; and
 - 4.1.2.3. not infringe any IPR.

5. Provision of ICT Services

- 5.1. The Supplier shall:
 - 5.1.1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;
 - 5.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;
 - 5.1.3. ensure that the Supplier System will be free of all encumbrances;
 - 5.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;
 - 5.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

6. Standards and Quality Requirements

- 6.1. The Supplier shall develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**").

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

- 6.2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.
- 6.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.
- 6.4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:
 - 6.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;
 - 6.4.2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and
 - 6.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

7. ICT Audit

- 7.1. The Supplier shall allow any auditor access to the Supplier premises to:
 - 7.1.1. inspect the ICT Environment and the wider service delivery environment (or any part of them);
 - 7.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;
 - 7.1.3. review the Supplier's quality management systems including all relevant Quality Plans.

8. Maintenance of the ICT Environment

- 8.1. If specified by the Buyer in the Order Form, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.
- 8.2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.
- 8.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance.
- 8.4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such

a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

9. Intellectual Property Rights in ICT

9.1. Assignments granted by the Supplier: Specially Written Software

9.1.1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:

9.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and

9.1.1.2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").

9.1.2. The Supplier shall:

9.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;

9.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and

9.1.2.3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the

full benefits of ownership of the Specially Written Software and New IPRs.

9.1.3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

9.2. Licences for non-COTS IPR from the Supplier and third parties to the Buyer

9.2.1. Unless the Buyer gives its Approval the Supplier must not use any:

- a) of its own Existing IPR that is not COTS Software;
- b) third party software that is not COTS Software

9.2.2. Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grants to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Central Government Body, any other Central Government Body's) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Call Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

9.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

9.2.3.1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and

9.2.3.2. only use such third party IPR as referred to at paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

9.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

9.2.5. The Supplier may terminate a licence granted under paragraph 9.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if

capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

9.3. Licenses for COTS Software by the Supplier and third parties to the Buyer

- 9.3.1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
- 9.3.2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
- 9.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licensee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
- 9.3.4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:
 - 9.3.4.1. will no longer be maintained or supported by the developer; or
 - 9.3.4.2. will no longer be made commercially available

9.4. Buyer's right to assign/novate licences

- 9.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 9.2 (to:
 - 9.4.1.1. a Central Government Body; or
 - 9.4.1.2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.
- 9.4.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 9.2.

9.5. Licence granted by the Buyer

- 9.5.1. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this

Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).

9.6. Open Source Publication

9.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

9.6.1.1. suitable for publication by the Buyer as Open Source; and

9.6.1.2. based on Open Standards (where applicable),

and the Buyer may, at its sole discretion, publish the same as Open Source.

9.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:

9.6.2.1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;

9.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;

9.6.2.3. do not contain any material which would bring the Buyer into disrepute;

9.6.2.4. can be published as Open Source without breaching the rights of any third party;

9.6.2.5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and

9.6.2.6. do not contain any Malicious Software.

9.6.3. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:

- 9.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and
- 9.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

9.7. Malicious Software

- 9.7.1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.
- 9.7.2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.
- 9.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.7.2 shall be borne by the Parties as follows:
 - 9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and
 - 9.7.3.2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

10. [Supplier-Furnished Terms

10.1. Software Licence Terms

- 10.1.1.1. Terms for licensing of non-COTS third party software in accordance with Paragraph 9.2.3 are detailed in [insert reference to relevant Schedule].
- 10.1.1.2. Terms for licensing of COTS software in accordance with Paragraph 9.3 are detailed in [insert reference to relevant Schedule].

10.2. Software as a Service Terms

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

10.2.1.1. Additional terms for provision of a Software as a Service solution are detailed in [insert reference to relevant Schedule].

10.3. Software Support & Maintenance Terms

10.3.1.1. Additional terms for provision of Software Support & Maintenance Services are detailed in [insert reference to relevant Schedule]]

Call-Off Schedule 7 (Key Supplier Staff)

- 1.1 The Order Form lists the key roles (“**Key Roles**”) and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.
- 1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.
- 1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.
- 1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:
 - 1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
 - 1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or
 - 1.4.3 the person’s employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.
- 1.5 The Supplier shall:
 - 1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

- 1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
 - 1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least three (3) Months' notice;
 - 1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and
 - 1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.
- 1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

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

Definitions

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

"BCDR Plan"	has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	has the meaning given to it in Paragraph 2.3.2 of this Schedule;
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable);

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

"Disaster Recovery Deliverables"	the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	has the meaning given to it in Paragraph 6.3 of this Schedule; and
"Supplier's Proposals"	has the meaning given to it in Paragraph 6.3 of this Schedule;

BCDR Plan

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

At least ninety (90) Working Days prior to the Start 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:

ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and

the recovery of the Deliverables in the event of a Disaster

The BCDR Plan shall be divided into three sections:

Section 1 which shall set out general principles applicable to the BCDR Plan;

Section 2 which shall relate to business continuity (the "**Business Continuity Plan**"); and

Section 3 which shall relate to disaster recovery (the "**Disaster Recovery Plan**").

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.

General Principles of the BCDR Plan (Section 1)

Section 1 of the BCDR Plan shall:

- set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;
- provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;
- contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;
- 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;
- 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;
- contain a risk analysis, including:
 - failure or disruption scenarios and assessments of likely frequency of occurrence;
 - identification of any single points of failure within the provision of Deliverables and processes for managing those risks;
 - identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and
- a business impact analysis of different anticipated failures or disruptions;
- provide for documentation of processes, including business processes, and procedures;
- set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;
- identify the procedures for reverting to "normal service";
- 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;
- identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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.

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

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

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

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

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

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

The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI's) or Service levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

Business Continuity (Section 2)

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 Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:

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

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

The Business Continuity Plan shall:

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

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 Deliverables;

specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and

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

Disaster Recovery (Section 3)

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.

The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:

- loss of access to the Buyer Premises;
- loss of utilities to the Buyer Premises;
- loss of the Supplier's helpdesk or CAFM system;
- loss of a Subcontractor;
- emergency notification and escalation process;
- contact lists;
- staff training and awareness;
- BCDR Plan testing;
- post implementation review process;
- any applicable Performance Indicators (PI's) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;
- 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;
- access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and
- testing and management arrangements.

Review and changing the BCDR Plan

The Supplier shall review the BCDR Plan:

- on a regular basis and as a minimum once every six (6) Months;
- within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 7; and

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 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.

Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.

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.

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.

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 Deliverables.

Testing the BCDR Plan

The Supplier shall test the BCDR Plan:

regularly and in any event not less than once in every Contract Year;
in the event of any major reconfiguration of the Deliverables
at any time where the Buyer considers it necessary (acting in its sole discretion).

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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.

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.

The Supplier shall ensure that any use by it or any Subcontractor 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.

The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:

- the outcome of the test;

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

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

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.

Invoking the BCDR Plan

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.

Circumstances beyond your control

The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.

Call-Off Schedule 9 (Security)

Long Form Security Requirements

Definitions

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

"Breach of Security"	<p>means the occurrence of:</p> <p>any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or</p> <p>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,</p> <p>in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;</p>
"ISMS"	<p>the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and</p>
"Security Tests"	<p>tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.</p>

Security Requirements

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.

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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

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

[insert security representative of the Buyer]

[insert security representative of the Supplier]

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

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

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

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

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

Information Security Management System (ISMS)

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

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

The Buyer acknowledges that;

If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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

The ISMS shall:

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

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

at all times provide a level of security which:

is in accordance with the Law and this Contract;

complies with the Baseline Security Requirements;

as a minimum demonstrates Good Industry Practice;

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

complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4)

(<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>)

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

complies with HMG Information Assurance Maturity Model and Assurance Framework

(<https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm>)

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

addresses issues of incompatibility with the Supplier's own organisational security policies; and

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

document the security incident management processes and incident response plans;

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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

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

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

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

If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable 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 the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

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

Security Management Plan

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

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

The Security Management Plan shall:

- be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);
- comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;
- identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;
- detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;
- unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
- set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);
- demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);
- set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;
- set out the scope of the Buyer System that is under the control of the Supplier;

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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

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

If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable 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 the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

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

Amendment of the ISMS and Security Management Plan

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

- emerging changes in Good Industry Practice;
- any change or proposed change to the Supplier System, the Deliverables and/or associated processes;
- any new perceived or changed security threats;
- where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;
- any new perceived or changed security threats; and
- any reasonable change in requirement requested by the Buyer.

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

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

suggested improvements to the effectiveness of the ISMS;
updates to the risk assessments;
proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and
suggested improvements in measuring the effectiveness of controls.

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

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

Security Testing

The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

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

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

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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

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

Complying with the ISMS

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

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

If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

Security Breach

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

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

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

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

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

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

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

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

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

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

Vulnerabilities and fixing them

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

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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

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

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

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

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

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

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

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

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

- is agreed with the Buyer in writing.

The Supplier shall:

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

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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

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

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

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

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

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

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

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

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

Part B – Annex 1:

Baseline security requirements

Handling Classified information

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

End user devices

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

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

Data Processing, Storage, Management and Destruction

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

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

The Supplier shall:

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

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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

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

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

Ensuring secure communications

The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.

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

Security by design

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

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

Security of Supplier Staff

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

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

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

All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

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

Restricting and monitoring access

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

Audit

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

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

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

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

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

Part B – Annex 2 - Security Management Plan

Call-Off Schedule 10 (Exit Management)

Definitions

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

"Exclusive Assets"	Supplier Assets used exclusively by the Supplier [or a Key Subcontractor] in the provision of the Deliverables;
"Exit Information"	has the meaning given to it in Paragraph 3.1 of this Schedule;
"Exit Manager"	the person appointed by each Party to manage their respective obligations under this Schedule;
"Exit Plan"	the plan produced and updated by the Supplier during the Initial Period in accordance with Paragraph 4 of this Schedule;
"Net Book Value"	the current net book value of the relevant Supplier Asset(s) calculated in accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice);
"Non-Exclusive Assets"	those Supplier Assets used by the Supplier [or a Key Subcontractor] in connection with the Deliverables but which are also used by the Supplier [or Key Subcontractor] for other purposes;
"Registers"	the register and configuration database referred to in Paragraph 2.2 of this Schedule;
"Replacement Goods"	any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

"Replacement Services"	any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Termination Assistance"	the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice;
"Termination Assistance Notice"	has the meaning given to it in Paragraph 5.1 of this Schedule;
"Termination Assistance Period"	the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule;
"Transferable Assets"	Exclusive Assets which are capable of legal transfer to the Buyer;
"Transferable Contracts"	Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation;
"Transferring Assets"	has the meaning given to it in Paragraph 8.2.1 of this Schedule;
"Transferring Contracts"	has the meaning given to it in Paragraph 8.2.3 of this Schedule.

Supplier must always be prepared for contract exit

The Supplier shall within 30 days from the Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.

During the Contract Period, the Supplier shall promptly:

create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables

("Registers").

The Supplier shall:

ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and

procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

Each Party shall appoint an Exit Manager within three (3) Months of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

Assisting re-competition for Deliverables

The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "**Exit Information**").

The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

Exit Plan

The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

The Exit Plan shall set out, as a minimum:

a detailed description of both the transfer and cessation processes, including a timetable;

how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;

details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;

proposals for the disposal of any redundant Deliverables and materials;

how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

The Supplier shall:

maintain and update the Exit Plan (and risk management plan) no less frequently than:

every [six (6) months] throughout the Contract Period; and

no later than [twenty (20) Working Days] after a request from the Buyer for an up-to-date copy of the Exit Plan;

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than [ten (10) Working Days] after the date of the Termination Assistance Notice;

as soon as reasonably possible following, and in any event no later than [twenty (20) Working Days] following, any material change to the Deliverables (including all changes under the Variation Procedure); and

jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

Termination Assistance

The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a "**Termination Assistance Notice**") at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

the nature of the Termination Assistance required; and

the start date and initial period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the End Date.

The Buyer shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:

no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and

the Buyer shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.

The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.

In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

Termination Assistance Period

- Throughout the Termination Assistance Period the Supplier shall:
- continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;
 - provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;
 - use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;
 - subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;
 - at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;
 - seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.
- If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.
- If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

Obligations when the contract is terminated

- The Supplier shall comply with all of its obligations contained in the Exit Plan.
- Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:
- vacate any Buyer Premises;
 - remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

such information relating to the Deliverables as remains in the possession or control of the Supplier; and

such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

Assets, Sub-contracts and Software

Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or

(subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");

which, if any, of:

the Exclusive Assets that are not Transferable Assets; and

the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the "**Transferring Contracts**"),

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.

Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.

Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:

procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which

procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.

The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.

The Buyer shall:

accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

No charges

Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

Dividing the bills

All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

the amounts shall be annualised and divided by 365 to reach a daily rate;

the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

Call-Off Schedule 13 (Implementation Plan and Testing)

Part A - Implementation

definitions

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

"Delay"	a) a delay in the Achievement of a Milestone by its Milestone Date; or b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
"Deliverable Item"	1 an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan;
"Milestone Payment"	2 a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone;
Implementation Period"	3 has the meaning given to it in Paragraph 7.1;

Agreeing and following the Implementation Plan

A draft of the Implementation Plan is set out in the Annex to this Schedule.
The Supplier shall provide a further draft Implementation Plan [**Insert** number of days] days after the Call-Off Contract Start Date.

The draft Implementation Plan:

must contain information at the level of detail necessary to manage the implementation stage effectively and as the Buyer may otherwise require; and

it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.

Following receipt of the draft Implementation Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the Implementation Plan. If the Parties are unable to agree the contents

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

of the Implementation Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is Achieved on or before its Milestone Date.

The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.

Reviewing and changing the Implementation Plan

Subject to Paragraph 4.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer's instructions and ensure that it is updated on a regular basis.

The Buyer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

Changes to any Milestones, Milestone Payments and Delay Payments shall only be made in accordance with the Variation Procedure.

Time in relation to compliance with the Implementation Plan shall be of the essence and failure of the Supplier to comply with the Implementation Plan shall be a material Default.

Security requirements before the Start Date

The Supplier shall note that it is incumbent upon them to understand the lead-in period for security clearances and ensure that all Supplier Staff have the necessary security clearance in place before the Call-Off Start Date. The Supplier shall ensure that this is reflected in their Implementation Plans.

The Supplier shall ensure that all Supplier Staff and Subcontractors do not access the Buyer's IT systems, or any IT systems linked to the Buyer, unless they have satisfied the Buyer's security requirements.

The Supplier shall be responsible for providing all necessary information to the Buyer to facilitate security clearances for Supplier Staff and Subcontractors in accordance with the Buyer's requirements.

The Supplier shall provide the names of all Supplier Staff and Subcontractors and inform the Buyer of any alterations and additions as they take place throughout the Call-Off Contract.

The Supplier shall ensure that all Supplier Staff and Subcontractors requiring access to the Buyer Premises have the appropriate security clearance. It is the Supplier's responsibility to establish whether or not the level of clearance will be sufficient for access. Unless prior approval has been received from the Buyer, the Supplier shall be responsible for meeting the costs associated with the provision of security cleared escort services.

If a property requires Supplier Staff or Subcontractors to be accompanied by the Buyer's Authorised Representative, the Buyer must be given reasonable notice of such a requirement, except in the case of emergency access.

What to do if there is a Delay

If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:

- notify the Buyer as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;

- include in its notification an explanation of the actual or anticipated impact of the Delay;

- comply with the Buyer's instructions in order to address the impact of the Delay or anticipated Delay; and

- use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

Compensation for a Delay

If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Supplier shall pay to the Buyer such Delay Payments (calculated as set out by the Buyer in the Implementation Plan) and the following provisions shall apply:

- the Supplier acknowledges and agrees that any Delay Payment is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to Achieve the corresponding Milestone;

Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier's failure to Achieve a Milestone by its Milestone Date except where:

- the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (When CCS or the Buyer can end this contract); or

the delay exceeds the number of days (the "**Delay Period Limit**") specified in the Implementation Plan commencing on the relevant Milestone Date;

the Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is Achieved;

no payment or other act or omission of the Buyer shall in any way affect the rights of the Buyer to recover the Delay Payments or be deemed to be a waiver of the right of the Buyer to recover any such damages; and

Delay Payments shall not be subject to or count towards any limitation on liability set out in Clause 11 (How much you can be held responsible for).

[Implementation Plan

The Implementation Period will be a [six (6)] Month period.

During the Implementation Period, the incumbent supplier shall retain full responsibility for all existing services until the Call-Off Start Date or as otherwise formally agreed with the Buyer. The Supplier's full service obligations shall formally be assumed on the Call-Off Start Date as set out in Order Form.

In accordance with the Implementation Plan, the Supplier shall:

- work cooperatively and in partnership with the Buyer, incumbent supplier, and other Framework Supplier(s), where applicable, to understand the scope of Services to ensure a mutually beneficial handover of the Services;
- work with the incumbent supplier and Buyer to assess the scope of the Services and prepare a plan which demonstrates how they will mobilise the Services;
- liaise with the incumbent Supplier to enable the full completion of the Implementation Period activities; and
- produce a Implementation Plan, to be agreed by the Buyer, for carrying out the requirements within the Implementation Period including, key Milestones and dependencies.

The Implementation Plan will include detail stating:

- how the Supplier will work with the incumbent Supplier and the Buyer Authorised Representative to capture and load up information such as asset data ; and
- a communications plan, to be produced and implemented by the Supplier, but to be agreed with the Buyer, including the frequency, responsibility for and nature of communication with the Buyer and end users of the Services.

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

In addition, the Supplier shall:

- appoint a Supplier Authorised Representative who shall be responsible for the management of the Implementation Period, to ensure that the Implementation Period is planned and resourced adequately, and who will act as a point of contact for the Buyer;

- mobilise all the Services specified in the Specification within the Call-Off Contract;

- produce a Implementation Plan report for each Buyer Premises to encompass programmes that will fulfil all the Buyer's obligations to landlords and other tenants:

- the format of reports and programmes shall be in accordance with the Buyer's requirements and particular attention shall be paid to establishing the operating requirements of the occupiers when preparing these programmes which are subject to the Buyer's approval; and

- the Parties shall use reasonable endeavours to agree the contents of the report but if the Parties are unable to agree the contents within twenty (20) Working Days of its submission by the Supplier to the Buyer, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

- manage and report progress against the Implementation Plan;

- construct and maintain a Implementation risk and issue register in conjunction with the Buyer detailing how risks and issues will be effectively communicated to the Buyer in order to mitigate them;

- attend progress meetings (frequency of such meetings shall be as set out in the Order Form) in accordance with the Buyer's requirements during the Implementation Period.

- Implementation meetings shall be chaired by the Buyer and all meeting minutes shall be kept and published by the Supplier; and

- ensure that all risks associated with the Implementation Period are minimised to ensure a seamless change of control between incumbent provider and the Supplier.]

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

Annex 1: Implementation Plan

The Implementation Plan is set out below and the Milestones to be Achieved are identified below:

Milest one	Delive rable Items	Duration	Miles tone Date	Buyer Responsibil ities	Milestone Payments	Delay Payments
[]	[]	[]	[]	[]	[]	[]
<p>The Milestones will be Achieved in accordance with this Call-Off Schedule 13: (Implementation Plan and Testing)</p> <p>For the purposes of Paragraph 9.1.2 the Delay Period Limit shall be [insert number of days].</p>						

Part B - Testing

1. Definitions

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

"Component"	4 any constituent parts of the Deliverables;
"Material Test Issue"	5 a Test Issue of Severity Level 1 or Severity Level 2;
"Satisfaction Certificate"	6 a certificate materially in the form of the document contained in Annex 2 issued by the Buyer when a Deliverable and/or Milestone has satisfied its relevant Test Success Criteria;
"Severity Level"	7 the level of severity of a Test Issue, the criteria for which are described in Annex 1;
"Test Issue Management Log"	8 a log for the recording of Test Issues as described further in Paragraph 8.1 of this Schedule;
"Test Issue Threshold"	9 in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan;
"Test Reports"	10 the reports to be produced by the Supplier setting out the results of Tests;
"Test Specification"	11 the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph 6.2 of this Schedule;

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

Call-Off Ref:

Crown Copyright 2018

"Test Strategy"	12 a strategy for the conduct of Testing as described further in Paragraph 3.2 of this Schedule;
"Test Success Criteria"	13 in relation to a Test, the test success criteria for that Test as referred to in Paragraph 5 of this Schedule;
"Test Witness"	14 any person appointed by the Buyer pursuant to Paragraph 9 of this Schedule; and
"Testing Procedures"	15 the applicable testing procedures and Test Success Criteria set out in this Schedule.

2. How testing should work

- 2.1 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, Test Specification and the Test Plan.
- 2.2 The Supplier shall not submit any Deliverable for Testing:
 - 2.2.1 unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;
 - 2.2.2 until the Buyer has issued a Satisfaction Certificate in respect of any prior, dependant Deliverable(s); and
 - 2.2.3 until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).
- 2.3 The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.
- 2.4 Prior to the issue of a Satisfaction Certificate, the Buyer shall be entitled to review the relevant Test Reports and the Test Issue Management Log.

Framework Ref: RM6273 Employee Benefits and Services

Project Version: v1.0

2

Model Version: v3.1

3. Planning for testing

- 3.1 The Supplier shall develop the final Test Strategy as soon as practicable after the Start Date but in any case no later than twenty (20) Working Days after the Start Date.
- 3.2 The final Test Strategy shall include:
 - 3.2.1 an overview of how Testing will be conducted in relation to the Implementation Plan;
 - 3.2.2 the process to be used to capture and record Test results and the categorisation of Test Issues;
 - 3.2.3 the procedure to be followed should a Deliverable fail a Test, fail to satisfy the Test Success Criteria or where the Testing of a Deliverable produces unexpected results, including a procedure for the resolution of Test Issues;
 - 3.2.4 the procedure to be followed to sign off each Test;
 - 3.2.5 the process for the production and maintenance of Test Reports and a sample plan for the resolution of Test Issues;
 - 3.2.6 the names and contact details of the Buyer and the Supplier's Test representatives;
 - 3.2.7 a high level identification of the resources required for Testing including Buyer and/or third party involvement in the conduct of the Tests;
 - 3.2.8 the technical environments required to support the Tests; and
 - 3.2.9 the procedure for managing the configuration of the Test environments.

4. Preparing for Testing

- 4.1 The Supplier shall develop Test Plans and submit these for Approval as soon as practicable but in any case no later than twenty (20) Working Days prior to the start date for the relevant Testing as specified in the Implementation Plan.
- 4.2 Each Test Plan shall include as a minimum:
 - 4.2.1 the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being Tested

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

Call-Off Ref:

Crown Copyright 2018

and, for each Test, the specific Test Success Criteria to be satisfied; and

4.2.2a detailed procedure for the Tests to be carried out.

- 4.3 The Buyer shall not unreasonably withhold or delay its approval of the Test Plan provided that the Supplier shall implement any reasonable requirements of the Buyer in the Test Plan.

5. Passing Testing

- 5.1 The Test Success Criteria for all Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 4.

6. How Deliverables will be tested

- 6.1 Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least 10 Working Days prior to the start of the relevant Testing (as specified in the Implementation Plan).

- 6.2 Each Test Specification shall include as a minimum:

6.2.1 the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Buyer and the extent to which it is equivalent to live operational data;

6.2.2 a plan to make the resources available for Testing;

6.2.3 Test scripts;

6.2.4 Test pre-requisites and the mechanism for measuring them; and

6.2.5 expected Test results, including:

- (a) a mechanism to be used to capture and record Test results; and
- (b) a method to process the Test results to establish their content.

7. Performing the tests

- 7.1 Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.

Framework Ref: RM6273 Employee Benefits and Services

Project Version: v1.0

Model Version: v3.1

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

Call-Off Ref:

Crown Copyright 2018

- 7.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 9.3.
- 7.3 The Supplier shall notify the Buyer at least 10 Working Days in advance of the date, time and location of the relevant Tests and the Buyer shall ensure that the Test Witnesses attend the Tests.
- 7.4 The Buyer may raise and close Test Issues during the Test witnessing process.
- 7.5 The Supplier shall provide to the Buyer in relation to each Test:
 - 7.5.1 a draft Test Report not less than 2 Working Days prior to the date on which the Test is planned to end; and
 - 7.5.2 the final Test Report within 5 Working Days of completion of Testing.
- 7.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:
 - 7.6.1 an overview of the Testing conducted;
 - 7.6.2 identification of the relevant Test Success Criteria that have/have not been satisfied together with the Supplier's explanation of why any criteria have not been met;
 - 7.6.3 the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;
 - 7.6.4 the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in each case grouped by Severity Level in accordance with Paragraph 8.1; and
 - 7.6.5 the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.
- 7.7 When the Supplier has completed a Milestone it shall submit any Deliverables relating to that Milestone for Testing.
- 7.8 Each party shall bear its own costs in respect of the Testing. However, if a Milestone is not Achieved the Buyer shall be entitled to recover from the Supplier, any reasonable additional costs it may incur as a direct result of further review or re-Testing of a Milestone.

Framework Ref: RM6273 Employee Benefits and Services

Project Version: v1.0

Model Version: v3.1

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

Call-Off Ref:

Crown Copyright 2018

- 7.9 If the Supplier successfully completes the requisite Tests, the Buyer shall issue a Satisfaction Certificate as soon as reasonably practical following such successful completion. Notwithstanding the issuing of any Satisfaction Certificate, the Supplier shall remain solely responsible for ensuring that the Deliverables are implemented in accordance with this Contract.

8. Discovering Problems

- 8.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.
- 8.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Buyer upon request.
- 8.3 The Buyer shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

9. Test witnessing

- 9.1 The Buyer may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Buyer, each of whom shall have appropriate skills to fulfil the role of a Test Witness.
- 9.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.
- 9.3 The Test Witnesses:
- 9.3.1 shall actively review the Test documentation;
 - 9.3.2 will attend and engage in the performance of the Tests on behalf of the Buyer so as to enable the Buyer to gain an informed

Framework Ref: RM6273 Employee Benefits and Services

Project Version: v1.0

Model Version: v3.1

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

Call-Off Ref:

Crown Copyright 2018

view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;

9.3.3 shall not be involved in the execution of any Test;

9.3.4 shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;

9.3.5 may produce and deliver their own, independent reports on Testing, which may be used by the Buyer to assess whether the Tests have been Achieved;

9.3.6 may raise Test Issues on the Test Issue Management Log in respect of any Testing; and

9.4 may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

10. Auditing the quality of the test

10.1 The Buyer or an agent or contractor appointed by the Buyer may perform on-going quality audits in respect of any part of the Testing (each a "**Testing Quality Audit**") subject to the provisions set out in the agreed Quality Plan.

10.2 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.

10.3 The Buyer will give the Supplier at least 5 Working Days' written notice of the Buyer's intention to undertake a Testing Quality Audit.

10.4 The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Buyer to enable it to carry out the Testing Quality Audit.

10.5 If the Testing Quality Audit gives the Buyer concern in respect of the Testing Procedures or any Test, the Buyer shall prepare a written report for the Supplier detailing its concerns and the Supplier shall, within a reasonable timeframe, respond in writing to the Buyer's report.

10.6 In the event of an inadequate response to the written report from the Supplier, the Buyer (acting reasonably) may withhold a Satisfaction Certificate until the issues in the report have been addressed to the reasonable satisfaction of the Buyer.

Framework Ref: RM6273 Employee Benefits and Services

Project Version: v1.0

Model Version: v3.1

11. Outcome of the testing

- 11.1 The Buyer will issue a Satisfaction Certificate when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.
- 11.2 If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Buyer shall notify the Supplier and:
 - 11.2.1 the Buyer may issue a Satisfaction Certificate conditional upon the remediation of the Test Issues;
 - 11.2.2 the Buyer may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or
 - 11.2.3 where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.
- 11.3 The Buyer shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.
- 11.4 The Buyer shall issue a Satisfaction Certificate in respect of a given Milestone as soon as is reasonably practicable following:
 - 11.4.1 the issuing by the Buyer of Satisfaction Certificates and/or conditional Satisfaction Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and
 - 11.4.2 performance by the Supplier to the reasonable satisfaction of the Buyer of any other tasks identified in the Implementation Plan as associated with that Milestone.
- 11.5 The grant of a Satisfaction Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of any Implementation Plan and Clause 4 (Pricing and payments).

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

Call-Off Ref:

Crown Copyright 2018

- 11.6 If a Milestone is not Achieved, the Buyer shall promptly issue a report to the Supplier setting out the applicable Test Issues and any other reasons for the relevant Milestone not being Achieved.
- 11.7 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Buyer shall issue a Satisfaction Certificate.
- 11.8 If there is one or more Material Test Issue(s), the Buyer shall refuse to issue a Satisfaction Certificate and, without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.
- 11.9 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Buyer may at its discretion (without waiving any rights in relation to the other options) choose to issue a Satisfaction Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:
 - 11.9.1 any Rectification Plan shall be agreed before the issue of a conditional Satisfaction Certificate unless the Buyer agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Buyer within 10 Working Days of receipt of the Buyer's report pursuant to Paragraph 10.5); and
 - 11.9.2 where the Buyer issues a conditional Satisfaction Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

12. Risk

- 12.1 The issue of a Satisfaction Certificate and/or a conditional Satisfaction Certificate shall not:
 - 12.1.1 operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Buyer's requirements for that Deliverable or Milestone; or
 - 12.1.2 affect the Buyer's right subsequently to reject all or any element of the Deliverables and/or any Milestone to which a Satisfaction Certificate relates.

Framework Ref: RM6273 Employee Benefits and Services

Project Version: v1.0

Model Version: v3.1

Annex 1: Test Issues – Severity Levels

1. Severity 1 Error

- 1.1 This is an error that causes non-recoverable conditions, e.g. it is not possible to continue using a Component.

2. Severity 2 Error

- 2.1 This is an error for which, as reasonably determined by the Buyer, there is no practicable workaround available, and which:
 - 2.1.1 causes a Component to become unusable;
 - 2.1.2 causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or
 - 2.1.3 has an adverse impact on any other Component(s) or any other area of the Deliverables;

3. Severity 3 Error

- 3.1 This is an error which:
 - 3.1.1 causes a Component to become unusable;
 - 3.1.2 causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or
 - 3.1.3 has an impact on any other Component(s) or any other area of the Deliverables;but for which, as reasonably determined by the Buyer, there is a practicable workaround available;

4. Severity 4 Error

- 4.1 This is an error which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Deliverables.

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

Call-Off Ref:

Crown Copyright 2018

5. Severity 5 Error

- 5.1 This is an error that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Deliverables.

Call-Off Ref:

Crown Copyright 2018

Annex 2: Satisfaction Certificate

To: [insert name of Supplier]

From: [insert name of Buyer]

[insert Date dd/mm/yyyy]

Dear Sirs,

Satisfaction Certificate

Deliverable/Milestone(s): [Insert relevant description of the agreed Deliverables/Milestones].

We refer to the agreement ("**Call-Off Contract**") [insert Call-Off Contract reference number] relating to the provision of the [insert description of the Deliverables] between the [*insert Buyer name*] ("**Buyer**") and [*insert Supplier name*] ("**Supplier**") dated [*insert Call-Off Start Date dd/mm/yyyy*].

The definitions for any capitalised terms in this certificate are as set out in the Call-Off Contract.

[We confirm that all the Deliverables relating to [insert relevant description of Deliverables/agreed Milestones and/or reference number(s) from the Implementation Plan] have been tested successfully in accordance with the Test Plan [or that a conditional

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

Call-Off Ref:

Crown Copyright 2018

Satisfaction Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria].

[OR]

[This Satisfaction Certificate is granted on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with Clause 4 (Pricing and payments)].

Yours faithfully

[insert Name]

[insert Position]

acting on behalf of [insert name of Buyer]

Call-Off Schedule 14 (Service Levels)

REDACTED

Framework Ref: RM6273 Employee Benefits and Services

Project Version: v1.0

Model Version: v3.1

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

1. Definitions

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

"Operational Board"	the board established in accordance with paragraph 4.1 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. Project Management

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager's shall be:

- 3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;**
- 3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;**
- 3.1.3 able to cancel any delegation and recommence the position himself; and**

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

Call-Off Ref:

Crown Copyright 2018

3.1.4 replaced only after the Buyer has received notification of the proposed change.

- 3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager's in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.
- 3.3 Receipt of communication from the Supplier's Contract Manager's by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. Role of the Operational Board

- 4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.
- 4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.
- 4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.
- 4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.
- 4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

Framework Ref: RM6273 Employee Benefits and Services

Project Version: v1.0

15

Model Version: v3.1

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

Call-Off Ref:

Crown Copyright 2018

5. Contract Risk Management

- 5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.
- 5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:
 - 5.2.1 the identification and management of risks;
 - 5.2.2 the identification and management of issues; and
 - 5.2.3 monitoring and controlling project plans.
- 5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.
- 5.4 The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer's and the Supplier have identified.

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

Call-Off Ref:

Crown Copyright 2018

Annex: Contract Boards

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

[**Guidance note:** Details of additional boards to be inserted.]

Call-Off Schedule 18 (Background Checks)

When you should use this Schedule

This Schedule should be used where Supplier Staff must be vetted before working on Contract.

Definitions

“Relevant Conviction” means any conviction listed in Annex 1 to this Schedule.

Relevant Convictions

The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.

Notwithstanding Paragraph 2.1.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):

carry out a check with the records held by the Department for Education (DfE);

conduct thorough questioning regarding any Relevant Convictions; and

ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),


and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

Annex 1 – Relevant Convictions

Not applicable

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract

 Intellectual Property Office	Project Title	Provision of Employee Benefits & Services
---	---------------	---

1.1 SUMMARY

The Intellectual Property Office (IPO) offers voluntary employee benefits. Our benefits offering is a key part of our wider Employee Value Proposition (EVP) which supports the achievement of Our Organisation strategic pillar where we strive to be high performing, with skilled people connected by shared purpose.

1.2 IPO needs to maintain a meaningful and diverse employee benefits offering to attract and retain our workforce and meet our long-term mission to help people grow the UK economy by providing an IP system that encourages investment in creativity and innovation.

1.3 The Intellectual Property Office (IPO) is seeking to provide a benefits platform to employees that includes:

1.3.1 Employee Discounts Scheme – a service from which IPO employees can access competitive discounts on goods and services at any time. This will include use of an App to save on the go.

1.3.2 Reward and Recognition scheme - the provision of an employee recognition system (both financial and non-financial) that enables peer to peer and manager to employee recognition, team recognition, with links to the discount scheme where required and with customisable recognition templates including standard templates for birthdays, long service, etc.

1.3.3 Home and Technology benefit - a service that allows employees to get instant access to free financing from their employer on the latest white goods and technology products and spread the cost over various periods.

1.3.4 Cycle to work scheme – a scheme that takes advantage of a tax exemption that allows the employer to loan cycles and cyclists' safety equipment to employees as a tax-free benefit.

1.3.5 Childcare vouchers. The IPO will require support with the operated Childcare voucher Schemes. Please see details in Sections 6.143 to Sections 6.147.

1.4 There may also be additional benefits that IPO does not currently offer which we would be interested in exploring with the potential supplier and we are open to expanding the scope of our offering if there are tangible benefits for both employees and the wider organisation, such as salary sacrifice for electric vehicles. Dental Insurance, Gym Discounts and Local Benefits.

2. BACKGROUND TO THE REQUIREMENT

2.1 The IPO is seeking a supplier to provide its employees with a high quality, employee benefits offering for the next 4 years. We already have in place various employee benefits that enhance our offering as a Civil Service employer, but we are looking for a provider that is innovative and can enhance existing provisions as well as provide new solutions for employees which are cost effective and benefit both individuals and the organisation.

2.2 The IPO employs approximately 1,700 people, the majority of which are located predominantly in our Newport Office. The employee base is diverse and geographically dispersed.

2.3 The IPO require a benefits solution that can be accessed by all employees wherever they undertake their work and at any time, 24 hours a day, 7 days a week and via an app.

2.4 The IPO is in the process of transforming our customer-facing services. This period of transformation has required significant investment over several years to date and is scheduled to continue into the early years of this contract. Hence, we are searching for the most cost effective solution to our benefits requirements over the next 4 years and where there are opportunities to improve value for money for the organisation and enhance the employee experience within our existing budgetary constraints, we would welcome detailed proposals.

3. DEFINITIONS

Expression/Acronym	Definition
IPO	Intellectual Property Office
DSIT	Department for Science, Innovation and Technology
EVP	Employee Value Proposition
IP	Intellectual Property
NCSC	The National Cyber Security Centre
Election Window	A finite period of time when sign up to a benefit is made possible for an individual.
24/7	Ongoing for twenty four hours a day, seven days a week
SMS	Short Message Service

5 AIMS, IMPLEMENTATION & CONTRACT

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

Crown Copyright 2018

- 5.1** The aim of this exercise is to procure a Potential Supplier to manage and administer an online employee benefits platform for the IPO that enhances the current offering whilst providing a cost-effective solution for the organisation.
- 5.2** The Potential Supplier must provide (and agree with the IPO) a clear step-by-step implementation plan. The plan must provide for the testing and delivery of the Online Employee Benefits Platform and associated functionality (as outlined in Section 6) to the IPO within 2 weeks of award of contract.
- 5.3** The implementation plan shall include, but not be limited to:
 - 5.3.1** Configuration of the Online Employee Benefits Platform (including branding, employee registration and log-on).
 - 5.3.2** testing the digital service with employees and iterating the service in line with employee needs.
 - 5.3.3** data security requirements; implementation plans for each of the benefits.
 - 5.3.4** IPO on-boarding and transition (including engagement with the IPO's internal payroll, communications and security teams).
 - 5.3.5** launch and promotion of the service to the IPO.
- 5.4** The resulting contract from this procurement will have a 'break clause' after the initial 15 months of the contract. This will permit the IPO (Intellectual Property Office) to terminate the contract by agreement after the first anniversary of the commencement date by giving written notice of termination of at least 60 days, to the desired termination date.
- 5.5** The potential supplier would have transition obligations upon termination as outlined in Section 6.6.

6 THE REQUIREMENT

- 6.1** The successful supplier will be expected to consistently demonstrate that they can provide best value and service throughout the term of the contract.
- 6.2** Responses should demonstrate how suppliers will support the IPO to continue to deliver a competitive and well utilised Employee Value Proposition (EVP).
- 6.3** Responses should demonstrate how suppliers will support the IPO's environmental ambition, by helping to create an EVP that means their employees can live and work more sustainably. This should include how they will engage with suppliers and products in the sustainable benefits field.
- 6.4** The IPO does not guarantee volumes, and the indicative volumes provided are subject to fluctuation, future policy changes and budgetary constraints.

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

Crown Copyright 2018

6.5 Full details of the proposed contract term is in the header above; however the IPO wish to initiate a positive, long term and effective relationship with the successful Potential Supplier.

6.6 Transition Management

6.7 Should the need arise, the potential supplier must ensure the efficient transfer of all IPO Occupational Health services and information provided under the contract to any new supplier(s).

6.8 A comprehensive transition plan must be delivered to and agreed by the IPO six weeks in advance of any change of provider.

6.9 Services must be implemented and stabilised, together with a communications strategy developed to ensure that the IPO is kept informed at key stages during the transition of services.

6.10 The service fees, where applicable, shall be reviewed annually on the contract anniversary and shall be based on the most recently available headcount data, provided by the IPO Pay and Reward Team.

6.11 Employee Discounts Scheme - the potential supplier shall provide employee discounts on a range of goods and services. These shall appeal to the diverse employee base of the IPO and shall include branded high street names as well as local offers.

6.12 Reward and Recognition Scheme – the supplier shall provide a reward and recognition scheme covering a range of loyalty, reward and recognition awards. The awards shall be made through vouchers and gift cards covering a range of goods and services and shall include branded high street names as well as local offers as requested by IPO.

6.13 Home and Technology Discount Scheme – the supplier shall provide technology and smartphone discounts to employees including discounts on the latest technology from leading manufacturers.

6.14 Cycle to Work Scheme – the supplier shall provide a facility for IPO employees to sacrifice part of their salary to loan cycles and cycle safety equipment for the main purpose of cycling to work.

6.15 The Online Employee Benefits Platform & IT Considerations

6.16 The Potential Supplier shall provide an IPO branded Online Employee Benefits Platform. This platform will allow for single sign on access to any other employee benefits that the IPO may have from other suppliers.

6.17 Features and Functionality

6.18 The Online Employee Benefits Platform shall be available 24/7, 365 days a year and have the following features:

- 6.19** Provide access to all benefits for permanent IPO employees e.g., retail discounts, salary sacrifice, reward and recognition. Agency staff shall be able to access retail discounts and reward and recognition elements only. Only employees on IPO payroll will be able to apply for any benefits that have payroll adjustments such as cycle to work, childcare and tech benefits. Contractors shall not have access to the benefits platform. However agency staff do have access to discount and signposting but are unable to access any salary sacrifice aspects (e.g. Home & Technology and Cycle to Work) as these individuals are paid by the agency and not via IPO payroll.
- 6.20** Be capable of providing users direct access to a third-party benefit providers website.
- 6.21** Must be a secure system and include a process to ensure that employees registering as users on the system are verified employees of the IPO.
- 6.22** Must provide the option for users to access the benefits portal and to receive communications and marketing using a personal email account. Use of a personal email account shall be permissible only after the user has been verified as an employee of the IPO. Any further system upgrades will only use the IPO email as a primary point of contact.
- 6.23** Must provide the option for users to opt out of any or all communications from the Supplier.
- 6.24** Must provide an interface with the IPO's systems as required, Contracting Authorities and HR/payroll system providers.
- 6.24.1** Must be able to do Single Sign On (SSO) to Entra ID. SAML2 preferred, other SSO methods can be considered.
- 6.24.2** Must be capable of User Provisioning from IPO. Entra SKIM preferred, other methods can be considered.
- 6.24.3** Desirable to have API access. For example to allow us to put in requests for vouchers through automated workflows.
- 6.25** Be configured to protect against fraud and that there is an option for the IPO to make system adaptations to meet organisational needs.
- 6.26** Must be capable of accepting uploads from IPO systems and of exporting data back to the IPO in an agreed format.
- 6.27** Must be capable of providing benefits during a monthly/annual 'Election Window' or as an anytime benefit. The dates of any election window shall be agreed with the IPO.
- 6.28** Must clearly display use of any cookies and an explanation of the meaning and working of cookies.
- 6.29** Must clearly state helpdesk contact details prior to user sign-in.

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

Crown Copyright 2018

- 6.30** It must be possible to enter, amend and delete details of users and their associated orders, voucher values, etc, in accordance with the Supplier and IPO's permissions as agreed at Call-Off Contract stage.
- 6.31** Must be possible to add/ delete and amend details of vouchers, goods and services and equipment from the range of options at a preferred IPO timeframe.
- 6.32** Must be capable of providing email confirmation to the user of the benefits selected and any transactions.
- 6.33** Must be capable of displaying options so that they are easily visible and displayed in a way that makes options clear and easy to compare.
- 6.34** Must be capable of providing an online audit trail to track the activity of users.
- 6.35** Must be capable of setting a limit on the value of the vouchers which can be ordered.
- 6.36** Must be capable of restricting the choice of benefits a user can take up in accordance with the IPO's policies and the benefits selected.
- 6.37** The Potential Supplier shall ensure that the Online Employee Benefits Platform has the capability to allow IPO users at any time- 24/7 - to allocate administrator roles which may include, but not limited to:
- 6.37.1** registering/de-registering users
 - 6.37.2** approving user requests
 - 6.37.3** amending user personal details
 - 6.37.4** viewing MI data/dashboards.
- 6.38** The Potential Supplier shall work with the IPO to ensure that reports are provided to the Potential Supplier to confirm which employees should have access to order from and authorise each benefit. The IPO should have admin rights to access reports 24/7.
- 6.39** The Potential Supplier shall work with the IPO to define the required fields each administrator or user will need to complete when ordering.
- 6.40** The Potential Supplier shall note that the IPO may have policies in place regarding eligibility. Where this is the case, the system shall ensure that ineligible employees cannot select any disallowed benefits.
- 6.41** The Potential Supplier shall ensure compatibility testing is undertaken with the IPO to ensure the system is compatible with different web browsers organisations use, and that system software updates are maintained. This will need to be undertaken and finalised at the earliest opportunity and within 5 weeks of contract award at the very latest.
- 6.42** The Potential Supplier shall ensure that all relevant terms and conditions are clearly displayed on the Online Employee Benefits Platform and that where any agreement is produced (for example a Cycle to Work salary sacrifice terms & conditions and financial eligibility of users prior to proceeding), a record is held for the life of the agreement and for a period thereafter to be agreed with the IPO.

- 6.43** The Potential Supplier shall ensure that documentation is readily available for the employee to view and/or print at zero cost and a copy must be available to the IPO.
- 6.44 Access** – The Supplier shall provide a 24/7 Online Employee Benefits Platform with a secure single sign on functionality to enable access to all the benefits. The service shall be closely integrated with internal systems to ensure a simple, seamless journey for all users.
- 6.45** The Potential Supplier shall ensure that the Online Employee Benefits Platform shall be accessible by users via the internet from work or home locations and via apps on both work and home mobile devices.
- 6.46** The Online Employee Benefits Platform shall be accessible through all internet devices – for example, laptops, mobile phones, and tablets, and shall be adjusted according to the device for easy navigation.
- 6.47** Access to the Online Employee Benefits Platform shall be through all internet browsers. The potential Supplier shall monitor access to ensure that the online employee benefits platform is accessible using any new technology that becomes available.
- 6.48** The Online Employee Benefits Platform shall adhere to the principles outlined in the Government Service Design Manual, NCSC Cloud Security Principles. The Potential Supplier shall allow access to the online benefits platform in accordance with the IPO's security policies.
- 6.49** If the Supplier's Online Employee Benefits Platform contains web access for employees, appropriate controls must be in place to ensure that individual employees are only able to access and review details of their own benefits arrangements. It must be possible to limit access to the Online Employee Benefits Platform, services and application by function and role. For example: controls will be required if IPO employees were to be provided with access in respect of report production or for other functions for example housekeeping, maintenance of drop-down tables, etc.
- 6.50 Maintenance and Upgrades** – The Potential Supplier shall ensure that full user testing is undertaken with the IPO to ensure that the platform is fully operational and meets the requirements of the IPO before any 'go live' date. The 'go live' date will be agreed with the IPO and the Potential Supplier must have a team to support the IPO / provide fixes should there be any initial issues.
- 6.51** The Potential Supplier must ensure that scheduled supplier system maintenance and system upgrades are implemented as soon as is practicable. Maintenance and system upgrades:
- 6.51.1** Must be provided by the Potential Supplier at no additional cost and with advance warning (notice period to the IPO of at least 4 weeks) including full user instructions if required.
- 6.51.2** Must occur outside the hours of 07:30 to 20:00 GMT (or BST as appropriate) Monday to Friday; and

- 6.51.3** Must be tested via the IPO networks prior to the upgrade version release going live. The Supplier shall inform the IPO of the key benefits of system upgrades as appropriate and in advance of the action being taken.
- 6.51.4** Must be tested via the IPO networks prior to the upgrade version release going live. The Supplier shall inform the IPO of the key benefits of system upgrades as appropriate and in advance of the action being taken.
- 6.52** The Potential Supplier must ensure that notification of scheduled maintenance and/or system upgrades is provided to IPO lead contacts which will be provided at the inception meeting with the successful supplier. A message shall be placed on the online employee Benefits Platform at least 2 weeks in advance of scheduled maintenance taking place, followed by subsequent reminders 48 and 24 hours prior to the maintenance occurring.
- 6.53** For upgrades that involve more extensive work, the Potential Supplier will notify the IPO lead at least 3 months in advance to enable us to adequately plan for any disruption and communicate changes to employees in advance, managing expectations and minimising loss of service.
- 6.54** If any supporting action is required by the IPO to assist the Potential Supplier with a system upgrade, the Potential Supplier must provide full details of the required assistance at least 6 weeks in advance.
- 6.55** **Employee Discount Scheme**
- 6.56** **Scheme information** - An Employee Discount Scheme allows IPO to offer invaluable money-saving opportunities to our employees by allowing them to take advantage of meaningful discounts on an extensive range of goods and services.
- 6.57** **Mandatory Requirements** - The Supplier shall provide through a fully automated system, a simple to operate, comprehensive Employee Discount Scheme where IPO employees can take advantage of discounts on a range of goods and services.
- 6.58** The Potential Supplier shall ensure that the range of products and services on offer via discounts, retail vouchers, online savings, and cashbacks appeal to the diverse employee base of the IPO and its employees to support our sustainability ambitions.
- 6.59** The Potential Supplier shall ensure that the scheme offers a sustainable and wide range of established, branded products and services as well as local discounts including any sourced by IPO at attractive, discounted rates from an extensive range of retailers and service providers
- 6.60** The Potential Supplier shall ensure that the range of products and services available shall include offers such as, but not limited to, discounts on supermarket shopping, food and drink, entertainment, cinema and leisure, health and wellbeing, holiday and travel, retail vouchers, cashback, and discount cards.
- 6.61** The Potential Supplier shall ensure that the cashback savings can be used against purchases on the Supplier's employee discounts site.

6.62 The Potential Supplier shall issue employees (at no cost to the IPO) with a replacement paper voucher, re-loadable electronic top up card, electronic print off voucher, SMS voucher or a refund if any Company they have purchased vouchers for ceases to accept the voucher and/or ceases to trade.

6.63 **Discounts** – The Potential Supplier’s discounts offerings must comply with the following requirements:

6.63.1 Ensure the discounts offered are competitive compared with similar Employee Benefits Schemes in the market and provide comparison data to the IPO as requested or as part of the review meetings.

6.63.2 Be able to offer a range of special offers, including seasonal offers that are better value than the usual discount offer.

6.63.3 Record and manage any cashback that an employee has earned online in dedicated accounts for employees that enables employees to use the funds against purchases on the site or to transfer the funds into their own personal bank account at any time.

6.63.4 Provide a range of re-loadable electronic top up cards, electronic print off vouchers, and SMS vouchers that can be purchased at less than face value, and dispatched at no cost to the employee, ensuring that as many discounts as possible are offered as an e-solution.

6.63.5 Ensure that the time taken to top up vouchers and gift cards shall be no longer than the retailers’ top up period.

6.63.6 Ensure that e-vouchers/instant vouchers are produced immediately.

6.63.7 Allow employees of the IPO and the IPO administrators to suggest local or regional companies to be incorporated in the scheme.

6.63.8 Support local businesses through offering a significant number of local and regional offers in addition to national offers and can negotiate directly with local and regional companies. The potential supplier should be able to incorporate existing local discounts or local discounts negotiated by the IPO onto their site at no additional cost.

6.64 **New Offers** – The Potential Supplier must:

6.64.1 Ensure that all offers available are kept up to date throughout the life of the contract.

6.64.2 Be able to source new products and services as requested by the IPO.

6.64.3 Research the market to source new and more competitive discounts and special offers.

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

Crown Copyright 2018

6.64.4 Continually monitor and review the uptake of offers to identify best sellers, with IPO agreement, remove, and replace those with low uptake and publicise new additions to the scheme.

6.64.5 Communicate with IPO before including any new offers on the site to inform them of the proposed offers allowing 7 days for them to veto the offering if they desire. IPO retains the absolute right to refuse to list or present certain offers or companies to their employees. The IPO may wish to refuse to list certain goods or services depending on the nature of their business.

6.64.6 Not make any offer or new product ranges available to the IPO and its employees until they have been approved to be offered.

6.64.7 Ensure that any changes are communicated to the IPO and additional communications shall be sent to employees.

6.65 Processing Requests – The Potential Supplier must:

6.65.1 Provide and maintain an employee discounts web page hosting online ordering.

6.65.2 Process all requests for cash back transfers so that it reaches the employee's bank account within 10 working days of the employee making a request or an alternative period specified by the IPO.

6.65.3 Allow employees to pay for discounts by either debit or credit cards. Any transaction fees associated with credit card payments shall be clearly shown to the employee against each purchase prior to completion of the transaction.

6.66 Reward and Recognition Scheme

6.67 Scheme Information:

6.68 The Reward and Recognition Scheme must provide IPO employees with access to a range of multi-choice, branded, high quality, loyalty, reward and recognition vouchers, external supplier sites and gift cards to nominated employees.

6.69 Loyalty, reward and recognition vouchers and gift cards can help fulfil IPO's objectives in a cost-efficient manner, as a motivator to ensure optimum productivity and staff retention. The awards made for exceptional individual and/or team performance, and potentially loyalty and service, need not be expensive since their symbolic value is greater than their monetary worth.

6.70 Reward and recognition vouchers and gift cards have been a popular choice for IPO employee incentive schemes as they are flexible and not only fit within budget but also allow the recipient to select their own gift.

6.71 Mandatory Requirements

6.72 The Potential Supplier shall provide on demand access to nominated (through an internal IPO 'Recognising Your Best' portal) users to vouchers, external supplier sites

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

Crown Copyright 2018

and gift cards that are redeemable at a wide range of outlets throughout the UK and online. The IPO would also like to explore the opportunity for local suppliers / outlets to be included in the reward & recognition voucher scheme.

6.73 The Potential Supplier shall ensure that a high-quality range of multi-choice rewards are available.

6.74 The Potential Supplier shall ensure that rewards are valid for a period specified by the IPO, from the date of the reward notification to the employee, to the date that the order for a voucher or gift card is placed.

6.75 The Potential Supplier shall make clear to the employee the period of validity of the award and any subsequent voucher or gift card against which it is redeemed.

6.76 The Potential Supplier shall ensure that the range of vouchers and gift cards on offer appeal to the diverse employee base of the IPO.

6.77 The Potential Supplier shall provide vouchers and gift cards to employees that are available in all formats provided by the retailer (e.g., physical gift cards and e-vouchers).

6.78 The Potential Supplier shall ensure the system meets the authorisation and invoicing requirements of the IPO and shall work closely with the IPO payroll team, Pay and Reward Team and Finance to deliver this. This includes setting up an authoriser based on specific data fields to be agreed with the IPO.

6.79 The Potential Supplier shall operate an efficient process for the payment of e-vouchers and gift cards. This must be instantly by email for E-vouchers and by 1st class mail for physical gift cards.

6.80 The Potential Supplier shall provide account information to support invoicing and to enable the IPO to develop their policy and monitor the success of their Reward and Recognition Scheme. This should be a line-by-line dataset showing each award. The content, format and frequency shall be specified by the IPO at successful supplier inception meeting.

6.81 The Supplier shall notify the IPO immediately and in advance if the organisational account is to be put on hold and provide the reasons for this. The Supplier shall provide sufficient notice to the IPO to enable the IPO to resolve the issue and minimise disruption for orders being processed.

6.82 The Potential Supplier shall provide the option for each administrator to personalise a 'Thank You' email to the employee of an award.

6.83 The Potential Supplier shall notify the IPO immediately if a retailer has ceased participation in offering vouchers and gift cards and withdraw availability of the option.

6.84 Ordering Process

6.85 The Potential Supplier shall ensure that all relevant data fields as specified by the IPO are completed in the required format on the Online Employee Benefits Platform prior

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

Crown Copyright 2018

to processing any order for vouchers or gift cards. The data fields, including any mandatory and non-mandatory fields, the format and number of required characters shall be specified by the IPO at call-off stage. The input fields are likely to include, but not limited to:

- 6.85.1** name of administrator/ordering officer
- 6.85.2** administrator's/ordering officer's work email address
- 6.85.3** administrator's/ordering officer's employee number
- 6.85.4** countersigning officer's name
- 6.85.5** countersigning officer's email address
- 6.85.6** countersigning officer's work email address
- 6.85.7** employee/recipient name
- 6.85.8** employee/recipient work email address
- 6.85.9** employee/recipient number
- 6.85.10** delivery Address
- 6.85.11** cost centre Code
- 6.85.12** purchase order number
- 6.85.13** retailer name
- 6.85.14** number of voucher(s) or gift cards(s)
- 6.85.15** value of voucher(s) or gift card(s)

6.86 Voucher Redemption – The Potential Supplier shall ensure that the vouchers and gift cards include but are not limited to:

- 6.86.1** accepted as full or part payment.
- 6.86.2** accepted throughout a wide range of Retail Outlets, Retail Groups, Specific Retailers and High Street Stores.
- 6.86.3** redeemable against entertainment events, outlets, and leisure attractions.
- 6.86.4** redeemable against hotel bookings.
- 6.86.5** redeemable for online purchases; and in person
- 6.86.6** refundable to the IPO, in the event, the retailer goes into receivership or ceases trading.

6.87 Voucher Value

6.88 The Potential Supplier shall ensure that the IPO is able to put a maximum and minimum cap on the amount that can be awarded to an employee according to our reward policies.

6.89 The Potential Supplier shall supply individual award vouchers and gift cards between the minimum and maximum value if specified by the IPO at Call-Off Contract stage.

6.90 The Potential Supplier shall provide all vouchers and gift cards in different denominations as offered by the retailer.

6.91 The Potential Supplier shall provide the option for the employee of the IPO to redeem the full value of the award from either one retailer or from multiple retailers.

6.92 The Potential Supplier shall notify the IPO of any change to the level of retailer discount as this becomes known and the date of any change in the offer to employees.

6.93 Lost or stolen orders, cancelling orders & expired orders

6.94 The Potential Supplier shall provide cover for lost or stolen orders up to the point of delivery to the delivery address, including if delivered to an incorrect postal or email address and shall have in place a system to provide replacement vouchers or gift cards at zero cost to the IPO or employee.

6.95 The Potential Supplier shall have in place procedures to provide replacement vouchers and gift cards at no extra cost where these have not been received by the employee if the voucher or gift card has not been redeemed.

6.96 The Potential Supplier shall provide the option for the IPO to cancel orders for recognition vouchers and gift cards prior to issue at zero cost to the IPO.

6.97 The Potential Supplier must refund or credit back to the IPO any cost of vouchers that expire after 12 months (normally).

6.98 The Potential Supplier shall be able to track and report (to the IPO and IPO employee) on the status of orders.

6.99 The Potential Supplier shall handle enquiries from IPO administrators giving information as to the status (tracking and processing) of their orders.

6.100 Non-Financial/Social Recognition

6.101 Social recognition is a form of employee recognition, that shows appreciation to an individual with no monetary value attached. Social recognition, or peer-to-peer recognition, is the act of employees empowering and acknowledging one another for great work. It is a meaningful source of motivation and, when it is a company habit, it becomes the backbone to an inclusive and collaborative working environment. The result is a sense of belonging, purpose, and achievement throughout the workforce.

6.102 The Potential Supplier shall provide a social recognition program with IPO bespoke branding that will allow anyone in the IPO to share experiences, award achievements, and extend congratulations to a colleague within the organisation.

6.103 Mandatory Requirements

6.104 The Potential Supplier shall provide on demand access for all IPO employees to a range of bespoke e-cards.

6.105 The Potential Supplier shall provide a social recognition program with IPO bespoke branding that will allow anyone in the IPO to share experiences, award achievements, and extend congratulations to a colleague across the organisation.

6.106 The Potential Supplier shall ensure that a high-quality range of multi-choice ecards are available.

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

Crown Copyright 2018

- 6.107** The Potential Supplier shall ensure that the range of e-cards on offer appeal to the diverse employee base of the IPO.
- 6.108** The Potential Supplier shall provide account information to support full reporting of e-cards including the ability to show results across the IPO that can be drilled down to an individual to allow evaluation and to monitor the success of the recognition scheme. This should be a line-by-line dataset showing each award. The content, format and frequency shall be specified by the IPO at the inception meeting for the successful supplier.
- 6.109** The Potential Supplier shall notify the IPO immediately and in advance – 48 hours minimum if the organisational account is to be put on hold and provide the reasons for this. The Potential Supplier must receive acknowledgment from the IPO Admin Team before the account is placed on hold and an agreed resolution process is in place. The Potential Supplier shall provide sufficient notice to the IPO to enable the IPO to resolve the issue and minimise disruption.
- 6.110** The Potential Supplier must be able to issue separate invoices for Purchases Orders that relate to differing business area requirements within IPO.
- 6.111** **Home and Technology Scheme**
- 6.112** **Scheme Information** - The Home and Technology scheme provides IPO employees with consumer technology and white goods discounts on the most up to date consumer products from leading manufacturers through retail outlets.
- 6.113** The scheme will provide the option for employees to use this scheme through, a net pay deduction option or as an employee discount option.
- 6.114** The Potential Supplier must be able to change the value limits and timeframe of any Home & Technology purchase through net pay deduction over the lifetime of the contract.
- 6.115** **Mandatory Requirements**
- 6.116** The Potential Supplier shall provide through a fully automated system, a simple to operate scheme for members to access, view and select technology and white goods discounts.
- 6.117** The Potential Supplier shall offer optional early leaver cover to guard against the occurrence of an employee leaving the organisation and exiting the scheme with payment outstanding where this is requested by the IPO. Details of this will be specified following the award of the contract.
- 6.118** The Potential Supplier shall provide a facility for employees to discuss their technology and needs and the options available, including specification details and suitability of the equipment to meet their needs.
- 6.119** The Potential Supplier shall provide insurance cover for loss or damage for products purchased through the scheme.

6.120 Promotion of the Home and Technology Scheme Service

- 6.121** The Potential Supplier shall work proactively with the IPO and promote the services at implementation stage and throughout the life of the agreement and any call-off contract.
- 6.122** The Potential Supplier shall be required to market and promote the services and provide promotional material at no additional cost to the IPO when required.
- 6.123** The Potential Supplier shall ensure regular promotion of all the services via paper and electronic means. This shall include, but not limited to webinars, live events, newsletters, posters, leaflets and emails. The Potential Supplier must ensure that communications are suitable and accessible to all employees.
- 6.124** The Potential Supplier must use management information and customer feedback to identify how the services are being utilised to assist in developing a promotion strategy for the IPO. The Potential Supplier shall continually assess the promotion strategy with the IPO at regular review meetings using the management information to identify areas to target.
- 6.125** The Potential Supplier shall conduct site visits primarily to the IPO Newport site and other relevant sites where necessary, to promote the services in accordance with industry practice. The Potential Supplier may also be required to attend specific or bespoke promotional events and roadshows at IPO's request. All these visits will be at the Potential Suppliers expense.
- 6.126** The Potential Supplier shall, when required attend customer network meetings to provide service up-dates, share good practice and develop new processes in order to drive consistency and promote collaboration.
- 6.127** The Potential Supplier shall provide a range of marketing tools designed to appeal to all groups of employees. This shall include information for new employees, guidance on how to use the Online Platform, the features and benefits, eligibility criteria, how to access and apply for the benefits and the potential savings.
- 6.128** The Potential Supplier shall promote the services through targeted marketing campaigns.
- 6.129** The Potential Supplier shall seek regular feedback from employees using online surveys, focus groups, etc. The specifics of these approaches must be agreed with the IPO.

6.130 Cycle to Work Scheme – Salary Sacrifice

- 6.131 Scheme Information** - The Cycle to Work scheme takes advantage of a tax exemption that allows the IPO to loan cycles and cyclists' safety equipment to employees as a tax-free benefit.

6.132 Mandatory Requirements

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

Crown Copyright 2018

- 6.133** The Potential Supplier must provide through a fully automated system, a simple to operate scheme for members to access, view and select a wide range of bicycles and cycle safety equipment.
- 6.134** The Potential Supplier must provide a facility for employees to discuss their cycle, related accessory needs and the options available, including specification details and suitability of the equipment to meet their needs.
- 6.135** The Potential Supplier must provide insurance cover for loss or damage for products purchased through the scheme.
- 6.136 Promotion of the Cycle to Work Service**
- 6.137** The Potential Supplier must work proactively with the IPO and promote the services at implementation stage and throughout the life of the contract period.
- 6.138** The Potential Supplier shall be required to market and promote the services and provide promotional material when required at no additional cost to the IPO.
- 6.139** The Potential Supplier shall ensure regular promotion of all the services via paper and electronic means. This must include, but not limited to webinars, live events, newsletters, posters, leaflets and emails. Potential Suppliers must ensure that all communications are suitable and accessible to all employees.
- 6.140** The Potential Supplier must use management information and customer feedback to identify how the services are being utilised to assist in developing a promotion strategy for the IPO. The Potential Supplier shall continually assess the promotion strategy with the IPO at regular review meetings using management information to identify areas to target.
- 6.141** The Potential Supplier will ensure that any unsubscribing from marketing communications will not affect service-related messages. For example individuals who are in a salary sacrifice agreement will receive notification regarding options from the supplier providing the goods about the end of hire options.
- 6.142** The Potential Supplier must be able to change the value limits and timeframe of the Cycle to Work scheme over the lifetime of the contract.
- 6.143 Childcare Vouchers.**
- 6.144** Childcare vouchers is a scheme that allows employees to use Salary Sacrifice to vary their contract of employment to give up part of their salary in return for childcare vouchers. IPO employees would legally agree to receive less pay in exchange for vouchers. The childcare vouchers can then be used to purchase childcare at a number of approved childcare providers nationwide. This is currently under a contract with another supplier, but we will need to migrate across to any potential new supplier.
- 6.145** This scheme was closed to new joiners from October 2018 so only has existing members within it. These vouchers are processed and paid via the suppliers portal and the salary sacrifice deductions are set up monthly on payroll. We currently have 14

members left in this scheme as of April 2025. Any potential new provider must be able to administer this scheme.

6.146 IPO Salary Plus Vouchers: This became payable from October 2018 for new joiners. We receive an application and then pay up to £20 per week (grossed up) into eligible parents pay. These payments are subject to tax / national insurance (NI) deductions though but rely heavily on parents telling us if they're no longer eligible. We have 76 members in receipt of these vouchers as of April 2025.

6.147 The IPO would like to explore the option of potentially processing the vouchers through payroll in order to collect tax and NI. This would allow payment to an approved / registered childcare provider as issuing vouchers for employees to use so will allow more governance of the process.

6.148 Employee Benefits Promotion and Engagement Activities:

6.149 The Potential Supplier shall be responsible for the effective promotion and ongoing employee engagement of the employee benefits portal and all associated services, discounts, and offers. To maximise awareness, usage, and overall value for money, the Potential Supplier must deliver a programme of promotional activities including quarterly 'roadshows'. The 'roadshows' may be required to be delivered virtually; however the IPO will require the Potential Supplier representatives to conduct site visits to the IPO Newport location and other relevant sites on a 6 monthly basis minimum, to promote the services in accordance with industry practice. The objective of the site visits and 'roadshows' would be to showcase the Employee Benefits Platform, explain new features, and highlight key offerings.

6.150 In addition to the scheduled quarterly events, the Potential Supplier shall deliver additional targeted promotional activities to align with seasonal periods or when launching new services, discount schemes, or enhancements.

6.151 These periods may include, but are not limited to, Christmas, Easter, the start of the financial year, and back-to-school seasons, where engagement opportunities and savings potential for employees are typically heightened.

6.152 The Potential Supplier must also ensure suitable promotional materials (e.g. posters, digital content, intranet banners, emails) are developed and made available to support internal communications and reach employees across different working environments, including those who are digitally or geographically remote.

6.153 Updates and Marketing:

6.154 The Potential Supplier shall, when required attend customer network meetings to provide service up-dates, share good practice and develop new processes in order to drive consistency and promote collaboration.

6.155 The Potential Supplier shall provide a range of marketing tools designed to appeal to all groups of employees. This shall include information for new employees, guidance on how to use the Online Platform, the features and benefits, eligibility criteria, how to access and apply for the benefits and the potential savings.

6.156 The Potential Supplier shall promote the services through targeted marketing campaigns.

6.157 The Potential Supplier shall seek regular feedback from employees using online surveys, focus groups, etc. These approaches shall be agreed with the IPO.

7. PROJECT MILESTONES

7.1 The Potential Supplier will note the following project milestones.

Milestone	Description	Timeframe
1	Start-up / Inception meeting via Microsoft Teams (or face to face if required)	Within 1 week of contract award
2	Implementation Plan provided & agreed with IPO.	Within 2 weeks of Contract Award
3	Test new processes & associated interfaces of Online Employee Benefits Platform. Onboard transition	Within 5 weeks of Contract Award
4	Launch and promotion of the service to the IPO	Within 6 weeks of Contract Award
5	Regular Review & Updates with Single Point of Contact Potential Supplier Team	Every month for the first quarter and thereafter every 3 months for the duration of the contract (or as IPO decree)
6	Liaison with the IPO Pay & Reward lead on a regular basis (to be agreed by IPO)	Ongoing during contract
7	Constant support with single point of Contact / account manager throughout the duration of the contract.	Ongoing during contract
8	Break Clause (optional)	After the initial 15 months of the contract.

8.1 SERVICE LEVELS & CUSTOMER SERVICE

8.2 The Potential Supplier must:

8.3 Provide a single point of contact (SPOC) who will be oversee and be accountable for the contract management team responsible for:

8.3.1 The performance of the contract and associated processes.

8.3.2 General contract management including adherence to an IPO Contract Management Plan (CMP) that will be shared and agreed with the Potential Supplier shortly after contract award.

8.3.3 Ongoing review of the CMP and assessment of performance against the plan.

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

Crown Copyright 2018

- 8.3.4** Act as an escalation point for any issues and provide updates on any escalations until resolution.
- 8.3.5** Attend regular review and contract management meetings
- 8.3.6** Manage the relationship with any of the Third Party Providers.

8.4 The Potential Supplier shall have in place a robust and auditable procedures for logging, investigating, managing, escalating and resolving complaints or problems initiated by the IPO and their employees. The procedure shall allow for the identification and tracking of individual complaints from initiation to resolution within the stipulated SLA's in the table below.

8.5 The Potential Supplier will provide the IPO with details of the process outlined in 8.4 resolution & issue resolution. The process must be agreed with the IPO.

8.6 Inform the IPO of changes in legislation, industry best practice and training standards.

8.7 Attend regular contract management reviews (including the facilitation of the attendance of their internal support teams, as required)

8.8 Track, monitor and report on progress through agreed KPIs.

8.9 Be responsible for Quality Assurance (QA) of the contract.

8.10 Identify opportunities and demonstrate continuous improvement throughout the lifetime of the contract.

8.11 Seek to reduce carbon emissions of delivery of this contract year on year.

8.12 The IPO will measure the quality of the Supplier's delivery by:

REDACTED

8.13 Typically, Management Information would include the following minimum data expectations:

8.13.1 Reward/Recognition Vouchers – Reports to include Award Value, Issue Date, Nominator, Nominee, Approver, Nomination ID (including nominee name, cost centre, staff no, organisation, grade, directorate) and Reason for nomination. Bespoke reporting capabilities with the ability to run by business directorate.

8.13.2 Retail Discounts – Reports to include MI on uptake of discount usage, total spend, savings made, and retailers used and employee IPO email address.

8.13.3 Home and Technology Benefit – Reports to include MI on uptake of technology benefit across IPO, including individual and total spend and most popular items.

8.13.4 Cycle to Work – Reports to include MI on update of Cycle to Work scheme across IPO.

9. OUTPUTS

- 9.1** The overall aim of the project is to obtain a bespoke benefits offering for IPO employees that is at least as favourable in terms of value as our current offering and where possible exceeds the package currently offered.
- 9.2** The benefits offering will be accessed by a fully supported electronic platform which will be compatible with IPO systems and access requirements.

10. TIMINGS

- 10.1** The contract for the current arrangement concludes on 31 October 2025 and another arrangement needs to be place and fully functional prior to this.
- 10.2** The Potential Supplier will need to provide an approved (by IPO) implementation plan, test any new processes & associated interfaces of the Online Employee Benefits Platform and onboard & transition launch and promotion of the service to the IPO well before the contract end date.

11. RESOURCES

- 11.1** While we have appropriate resources allocated in IPO to support the contract management of this arrangement, we envisage a large part of the administration relating to the management of this contract to be carried out on our behalf, by the Potential Supplier / Main Provider.
- 11.2** This contract will be managed by an IPO Contract Manager (supported by internal colleagues from across the organisation). Specifically, this IPO Contract Manager will:
- 11.2.1** Manage the overall relationship with the successful main supplier.
 - 11.2.2** Resolve issues such as delivery quality e.g., feedback, which cannot be resolved at area level, or is a serious breach.
 - 11.2.3** Arrange and lead monthly review meetings with the Main Provider.
 - 11.2.4** Provide technical updates and advice on changes within our organisation to the Main Provider.
 - 11.2.5** Oversee and seek assurances on quality of delivery.
 - 11.2.6** Consider contractual arrangements, amendments and extensions as appropriate.
 - 11.2.7** Manage a mechanism for a communication route between providers and operational areas.

12. VOLUMES

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

Crown Copyright 2018

- 12.1** The average volumes for the retail discounts for the 2024 calendar year under the current Supplier are illustrated in the table below.

Average IPO employee headcount/users	REDACTED
Average no. of employees logged in	REDACTED
Average % of employees logged in	REDACTED
Average no. of employees left to engage	REDACTED
Average monthly order value	REDACTED
Average monthly staff savings	REDACTED
Average monthly orders placed	REDACTED
Total average annual spend by IPO employees	REDACTED

- 12.2.** The IPO have targeted our communications over the last 18 months at improving take up and usage of the retail discounts portal and wider benefits and this has seen usage double in that time. We now have an embedded benefits offering which IPO employees are regularly using and we want to ensure that our future offering is as frequently used. We will want to work with the successful Supplier to maintain and improve take up of our benefits going forward.

13. CONFIDENTIALITY & IT SECURITY REQUIREMENTS

- 13.1** Confidentiality: The Potential Supplier will comply with clause 15 of the contract terms and conditions in respect of all work carried out for the customer.

- 13.2** All personal data processed must remain within the United Kingdom (UK) or the European Economic Area (EEA). The supplier shall ensure that no data is transferred outside these regions without prior written consent from the Intellectual Property Office (IPO).

- 13.3** The Potential Supplier shall not use any data provided by the IPO for the purpose of training artificial intelligence (AI) models. This includes, but is not limited to, machine learning algorithms, neural networks, and other AI technologies. The supplier must implement robust measures to ensure compliance with this requirement.

- 13.4** The Potential Supplier must comply with all applicable data protection laws and regulations, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The supplier shall ensure that appropriate technical and organisational measures are in place to protect personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage.

- 13.5** The Potential Supplier must ensure that all data is securely stored and processed, with encryption both in transit and at rest. Access to personal data must be restricted to authorised personnel only, and audit trails must be maintained to monitor data access and usage.

14. SUSTAINABILITY, SOCIAL VALUE, DIVERSITY/INCLUSION & IMPARTIALITY

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

Crown Copyright 2018

- 14.1** The IPO places significant importance on delivery and maximising social value commitments in accordance with the Government Commercial Function social value Model. Therefore there will be an evaluated tender question specific to social value within this Invitation to Tender.
- 14.2** The IPO has a responsibility to act and to support nature, the environment, and its vital contributions to biodiversity. The Supplier is required to act in sustainable manner in the delivery of the Contract, particularly in terms of eliminating waste, reducing travel and minimising energy consumption. The Supplier must comply with all current legislation regarding sustainability and legislation introduced or amended during the period of the contract pertaining to this.
- 14.3** This must include compliance with the Modern Slavery Act 2015 and the Climate Change Act 2008.
- 14.4** The Potential Supplier must consider their carbon footprint in allocating and deploying resources to undertake requirement.
- 14.5** The Potential Supplier shall ensure that all employees, subcontractors, agents, and any other personnel engaged in the delivery of this contract uphold the highest standards of professional behaviour at all times when interacting with IPO staff, service users, stakeholders, and members of the public.
- 14.6** The Potential Supplier must take all reasonable steps to prevent and address any instances of bullying, harassment, sexual harassment, victimisation, or unlawful discrimination on the grounds of protected characteristics as defined in the Equality Act 2010. This includes, but is not limited to, race, gender, disability, age, sexual orientation, religion or belief, and gender reassignment.
- 14.7** The Potential Supplier must promote a working environment that is inclusive, respectful, and free from offensive, inappropriate, or discriminatory language and behaviour. All staff engaged in the delivery of services under this contract are expected to demonstrate respect, courtesy, and professionalism in all communications and conduct.
- 14.8** The Potential Supplier must conduct all services and interactions under this contract with strict impartiality and neutrality. The Potential Supplier agrees to refrain from promoting, endorsing, or opposing any political, religious, or social ideologies in the course of fulfilling contractual obligations. All communications, deliverables, and representations must remain free from bias or influence that could compromise the perception or reality of neutrality, ensuring an inclusive and respectful environment for all stakeholders.

15 CONTINUOUS IMPROVEMENT

- 15.1** The Potential Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

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

Crown Copyright 2018

- 15.2** The Potential Supplier should present new ways of working to the IPO during monthly/quarterly Contract review meetings.
- 15.3** Changes to the way in which the Services are to be delivered must be brought to the IPO's attention and agreed prior to any changes being implemented.