Order Form

CALL-OFF REFERENCE:	WP2074.2 Outsourced Contact Centre Services
THE BUYER:	Government Digital Services
BUYER ADDRESS	The Whitechapel Building, 10 Whitechapel High Street, London E1 8QS
THE SUPPLIER:	Hinduja Global Solutions UK Ltd
SUPPLIER ADDRESS:	Vantage London Great West Road Brentford TW8 9AG
REGISTRATION NUMBER:	03017799
DUNS NUMBER:	777547712

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and is dated the date on which both parties have signed this Order Form (being the Start Date).

It is issued under the Framework Contract with the reference number RM6181 for the provision of Outsourced Contact Centre Services.

CALL-OFF LOT(S):
Lot 1 Contact Centres

CALL-OFF INCORPORATED TERMS
The following documents are incorporated into this Call-Off Contract. Where the words “NOT USED” appear we are not using those schedules. Where the word "REPLACED" appears there is a replacement Call Off Special Schedule. 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)
3. Paragraph 9 and Annex 2 of Framework Schedule 3 (Framework Prices).
4. Call Off Special Terms and (subject to Call Off Special Term 6) Call Off Special Schedules.

5. The following Schedules in equal order of precedence:

- Joint Schedules for **RM6181**
    - 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) [including Annex 5 – Optional Terms for Bronze Contracts]
    - Joint Schedule 8 (Guarantee) - NOT USED
    - Joint Schedule 9 (Minimum Standards of Reliability) - NOT USED
    - Joint Schedule 10 (Rectification Plan)
    - Joint Schedule 11 (Processing Data)
    - Joint Schedule 12 (Supply Chain Visibility)

- Call-Off Schedules for Call-Off reference number: 2074.2.
    - Call-Off Schedule 1 (Transparency Reports) – REPLACED
    - Call-Off Schedule 2 (Staff Transfer)
    - Call-Off Schedule 3 (Continuous Improvement) – REPLACED
    - 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) [amended for a Bronze Contract as per paragraph 10 of Part A of that Schedule]
    - Call-Off Schedule 9 (Security) - REPLACED
    - Call-Off Schedule 10 (Exit Management)
    - Call-Off Schedule 12 (Clustering) - NOT USED
    - Call-Off Schedule 11 (Installation Works)
    - Call-Off Schedule 13 (Implementation Plan and Testing) - REPLACED
    - Call-Off Schedule 14 (Service Levels) – REPLACED
    - Call-Off Schedule 15 (Call-Off Contract Management) – REPLACED
    - Call-Off Schedule 16 (Benchmarking)
    - Call-Off Schedule 17 (MOD Terms) - NOT USED
    - Call-Off Schedule 18 (Background Checks) - NOT USED
    - Call-Off Schedule 19 (Scottish Law) - NOT USED
    - Call-Off Schedule 20 (Call-Off Specification) – REPLACED
    - Call-off Schedule 21 (Northern Ireland Law) - NOT USED
    - Call-Off Schedule 22 (Lease Terms) - NOT USED
    - Call-Off Schedule 23 (HMRC Terms)
    - Call-Off Schedule 24 (Supplier Furnished Terms)

6. CCS PSC Outsourcing Core Terms (Version 1)
7. Joint Schedule 5 (Corporate Social Responsibility)
8. Call Off Special Schedule 3 (Supplier Solution) as long as any parts 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:

Special Term 1 - [redacted]

Special Term 2 – [redacted]

Special Term 3 – Where, within one year of the Start Date, it is identified that there has been any error in the Due Diligence Information provided by the Buyer to the Supplier, at the next meeting of the Operational and Service Review Board (as described in Call Off Special Schedule 8 (Call Off Contract Management)), the Operational and Service Review Board shall discuss and agree any adjustments required to the Contract and/or the Due Diligence Information as a result of such error and shall appoint representatives of each of the Buyer and the Supplier to implement those adjustments. If the Operational and Service Review Board cannot agree on the adjustments required, the matter shall be dealt with in accordance with the dispute resolution procedure set out in Clause 34 of the Core Terms.

Special Term 4 - Security

1. The Supplier shall engage and collaborate with GDS Security Working Group reviews led by Digital Identity security leads.

2. The Supplier shall comply with Call Off Special Schedule 1 (Security Management Schedule - Supplier Led Assurance). For the purposes of that schedule this Contract is a “higher- risk agreement”.

Special Term 5 - Data Protection

1. Paragraph 6(d) of Joint Schedule 11 shall be replaced with the following paragraph:

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

(i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 UK GDPR or section 74 of the DPA 2018;

(ii) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 DPA 2018) as determined by the Controller;

(iii) the Data Subject has enforceable rights and effective legal remedies;

(iv) 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

(v) 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”

Special Term 6 – Replacement Call-Off Schedules

1. The Parties agree that for the purpose of this Call-Off Contract the following Call Off Special Schedules shall replace the corresponding Call-Off Schedules in full:

Call Off Special Schedule	Call-Off Schedule Being Replaced
Call Off Special Schedule 1 – Security Management	Call-Off Schedule 9 – Security
Call Off Special Schedule 2 – Buyer Requirements	Call-Off Schedule 20 – Specification
Call Off Special Schedule 3 – Supplier Solution	Call-Off Schedule 4 – Call-Off Tender
Call Off Special Schedule 4 – Continuous Improvement	Call-Off Schedule 3 – Continuous Improvement
Call Off Special Schedule 5 – Implementation Plan and Testing	Call-Off Schedule 13 – Implementation Plan and Testing
Call Off Special Schedule 6 – Service Levels	Call-Off Schedule 14 – Service Levels
Call Off Special Schedule 7 – Pricing Details	Call-Off Schedule 5 – Pricing Details
Call Off Special Schedule 8 – Call Off Contract Management	Call-Off Schedule 15 – Call Off Contract Management

Call Off Special Schedule 9 – Transparency Reports	Call-Off Schedule 1 – Transparency Reports

2. For the purpose of the order of precedence set out on p2 above, the Call Off Special Schedules listed in the table above shall be treated as being the relevant Call-Off Schedules and not Call Off Special Schedules.

3. In this Call-Off Contract references to any Call-Off Schedule that is being replaced (as set out in the table above) shall be deemed to be references to the relevant Call Off Special Schedule.

CALL-OFF START DATE: The date on which both parties sign this Call-Off Contract.

CALL-OFF EXPIRY DATE: Three years from the Start Date.

CALL-OFF INITIAL PERIOD: 3 Years.

CALL-OFF OPTIONAL EXTENSION PERIOD
Up to two one-year periods.

CALL-OFF DELIVERABLES
See details in Call Off Special Schedule 2 (Buyer Requirements)

MAXIMUM LIABILITY
[redacted]

CALL-OFF CHARGES

Option B: See details in Call-Off Schedule 5 (Pricing Details)
All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices)

REIMBURSABLE EXPENSES

[redacted]

PAYMENT METHOD

[redacted]

BUYER'S INVOICE ADDRESS:

[redacted]

COLLABORATIVE WORKING PRINCIPLES

The Collaborative Working Principles apply to this Call-Off Contract.

FINANCIAL TRANSPARENCY OBJECTIVES

The Financial Transparency Objectives apply to this Call-Off Contract.

BUYER'S AUTHORISED REPRESENTATIVE

[redacted]

BUYER'S ENVIRONMENTAL POLICY

Please find below the link to the GDS sustainable development policy:
https://intranet.cabinetoffice.gov.uk/task/sustainable-development/

BUYER'S SECURITY POLICY

[redacted]

SUPPLIER'S AUTHORISED REPRESENTATIVE

[redacted]

SUPPLIER'S CONTRACT MANAGER

[redacted]

PROGRESS REPORT FREQUENCY

See Call Off Special Schedule 2 (Buyer Requirements), Section 2.15 Contract Management and Reporting.

PROGRESS MEETING FREQUENCY

Call Off Special Schedule 2 (Buyer Requirements), Section 2.15 Contract Management and Reporting.

STAFF TRANSFER - CALL OFF SCHEDULE 2

[redacted]

KEY STAFF

[redacted]

KEY SUBCONTRACTOR(S)

Key Contact / Named Representative: [redacted]

THE SUPPLIER: [redacted]

SUPPLIER ADDRESS: [redacted]

REGISTRATION NUMBER: [redacted]

DUNS NUMBER: [redacted]

COMMERCIALLY SENSITIVE INFORMATION

[redacted]

Document	Section	Supplier Reason for Redaction
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

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

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

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

SERVICE CREDITS

[redacted]

[redacted]

[redacted]

ADDITIONAL INSURANCES

[redacted]

GUARANTEE

[redacted]

SOCIAL VALUE COMMITMENT

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value requirements in Call Off Special Schedule 2 (Buyer Requirements).

PERSONAL DATA

The Parties agree that Annex 1 of Joint Schedule 11 (Processing Data) shall be replaced with the following:

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 are: [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 Relevant Authority is Controller and the Supplier is Processor The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: The Supplier will provide Contact Centre services for the Authority.
Duration of the Processing	For the duration of this Call-Off Contract.
Nature and purposes of the Processing	The Supplier will provide Contact Centre requirements for the Buyer which includes automated systems and direct contact between the citizen and the One Log in service.

Description	Details
Type of Personal Data	● Names ● Email address ● Home address ● Telephone number ● Date of Birth ● NI Numbers ● biometric data ● Identity Data
Categories of Data Subject	Citizens Administrative staff providing the service
Plan for return and destruction of the data once the Processing is complete **UNLESS requirement under Union or Member State law to preserve that type of data**	Data destruction and deletion to be agreed prior to exit of the contract and whereby the Buyer will instruct and identify the data sets appropriate for deletion within a year period for end of the contract. An assurance statement to be provided by the Supplier will be sought. This will include any data held by the Supplier on their own systems related to the Buyer data.

DEFINITIONS
In this Call-Off Contract the following terms shall have the following meanings:

Service Commencement Date	means the start date for the relevant operational Service once implementation and transition is complete and from which the Supplier is responsible for the delivery of the

	Service (in each case in accordance with this Call-Off Contract)
User	means an individual or entity that uses or interacts with the service to seek assistance, guidance or resolution from the customer support service, either through a customer support agent, team or representative (e.g. an automated system). The term can encompass various types of users, including end users who are UK citizens and government departments

Additional defined terms are set out in Joint Schedule 1 (Definitions and Interpretation) and elsewhere in this Contract.

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:		**Signature:**	
Name:		**Name:**	
Role:		**Role:**	
Date:		**Date:**	

Security Schedule: (Security Management: Supplier-led Assurance)

1 Buyer Options

1.1 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

Locations (see paragraph 1 of the Security Requirements)		
The Supplier and Sub-Contractors may store, access or Process Buyer Data in:	the United Kingdom only	✠
	the United Kingdom and European Economic Area only	☐
	anywhere in the world not prohibited by the Buyer	☐
Support Locations (see paragraph 1 of the Security Requirements)		
The Supplier and Sub-Contractors may operate Support Locations in:	the United Kingdom only	✠
	the United Kingdom and European Economic Area only	☐
	anywhere in the world not prohibited by the Buyer	☐
Locations for Development Activity (see paragraph 1 of the Security Requirements)		
The Supplier and Sub-Contractors may undertake Development Activity in:	the United Kingdom only	✠
	the United Kingdom and European Economic Area only	☐
	anywhere in the world not prohibited by the Buyer	☐

2 Definitions

"Anti-virus Software"	means software that: (a) protects the Supplier Information Management System from the possible introduction of Malicious Software; (b) scans for and identifies possible Malicious Software in the Supplier Information Management System; (c) if Malicious Software is detected in the Supplier Information Management System, so far as possible:

	(i) prevents the harmful effects of the Malicious Software; and (ii) removes the Malicious Software from the Supplier Information Management System;
"Buyer Data"	as defined in Schedule 1 (Definitions) means (a) the data (which shall include biometric data), text,drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Supplier by or on behalf of the Buyer; or (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; and (b) any Personal Data for which the Buyer is the Controller, and, for the avoidance of doubt, shall include any meta data relating to categories of data referred to in paragraphs (a) or (b), the Code and any meta data relating to the Code;
"Buyer Data Register"	means the register of all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer, produced and maintained in accordance with paragraph 15 of the Security Requirements;
"Buyer Premises"	as defined in Schedule 1 (Definitions);
"Buyer System"	means 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 Services;
"Breach Action Plan"	means a plan prepared under paragraph 14.3 of the Security Requirements addressing any Breach of Security;
"Breach of Security"	for the purposes of this Security Schedule, means the occurrence of: (a) any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Contract, including the Buyer Data and the Code; (d) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in connection with this Contract, including the Buyer Data and the Code; and/or

	(e) any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements; (f) the installation of Malicious Software in the: (i) Supplier Information Management System; (ii) Development Environment; or (iii) Developed System; (g) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the: (i) Supplier Information Management System; (ii) Development Environment; or (iii) Developed System; and (h) includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt: (i) was part of a wider effort to access information and communications technology by or on behalf of Central Government Bodies; or (ii) was undertaken, or directed by, a state other than the United Kingdom
"Certification Requirements"	means the requirements set out in paragraph 12.3.
"CHECK Scheme"	means the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks
"CHECK Service Provider"	means a company which, under the CHECK Scheme: (a) has been certified by the National Cyber Security Centre; (b) holds "Green Light" status; and (c) is authorised to provide the IT Health Check services required by paragraph 10 of the Security Requirements;
"Code"	means, in respect of the Developed System: (a) the Source code;

	(b) the Object code; (c) third-party components, including third-party coding frameworks and libraries; and (d) all supporting documentation.
"Code Review"	means a periodic review of the Code by manual or automated means to: (a) identify and fix any bugs; and (b) ensure the Code complies with (i) the requirements of this Security Schedule ; and (ii) the Secure Development Guidance;
"Code Review Plan"	means the document agreed with the Buyer under paragraph 5.2 of the Security Requirements setting out the requirements for, and frequency of, Code Reviews;
"Code Review Report"	means a report setting out the findings of a Code Review;
"Cyber Essentials"	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Plus"	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Scheme"	means the Cyber Essentials scheme operated by the National Cyber Security Centre;
"Developed System"	means any software or system that the Supplier will develop under this Contract either: (a) as part of the Services; or (b) to create or modify Software to: (i) provide the Services; or (ii) Process Buyer Data,;
"Development Activity"	means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including: (a) coding; (b) testing; (c) code storage; and (d) deployment.
"Development Environment"	means any information and communications technology system and the Sites forming part of the Supplier Information Management System that the Supplier or its Sub-contractors will use to provide the Development Activity;
"EEA"	means the European Economic Area;

"End-user Device"	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services.
"Email Service"	means a service that will send, or can be used to send, emails from the Buyer's email address or otherwise on behalf of the Buyer;
"Higher Risk Sub-contractor"	means a Sub-contractor that Processes Buyer Data, where that data includes either: (a) the Personal Data of 1000 or more individuals in aggregate during the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with Clause 4.1(b); or (b) any part of that Buyer Data includes any of the following: (i) financial information (including any tax and/or welfare information) relating to any person; (ii) any information relating to actual or alleged criminal offences (including criminal records); (iii) any information relating to children and/or vulnerable persons; (iv) any information relating to social care; (v) any information relating to a person's current or past employment; or (vi) Special Category Personal Data; or (c) the Buyer in its discretion, designates a Sub-contractor as a Higher Risk Sub-Contractor: (i) in any procurement document related to this Contract; or (ii) during the Term;
"HMG Baseline Personnel Security Standard"	means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 6.0, May 2018 (https://assets.publishing.service.gov.uk /government/uploads/system/uploads/attachment_data/file/714002/ HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf), as that document is updated from time to time;
"Independent Security Adviser"	means the independent and appropriately qualified and experienced security architect or expert appointed under Paragraph 18;

"Information Management System"	means the Supplier Information Management System and the Wider Information Management System;
"IT Health Check"	means testing of the Supplier Information Management System by a CHECK Service Provider;
International Data Transfer Agreement (IDTA's)	Replaces Standard Contract Clauses under UK GDPR for International data transfers/restricted data transfers, and processing of data outside the UK
"Malicious Software"	means 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;
"Medium Risk Sub-contractor"	means a Sub-contractor that Processes Buyer Data, [where that data (a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with Clause 4.1(b); and (b) does not include Special Category Personal Data;
"Modules Register"	means the register of Third-party Software Modules required by paragraph 7.2 of the Security Requirements;
"NCSC"	means the National Cyber Security Centre;
"NCSC Cloud Security Principles"	means the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles.
"NCSC Device Guidance"	means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;
"NCSC Protecting Bulk Personal Data Guidance"	means the NCSC's document "Protecting Bulk Personal Data", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data
"NCSC Secure Design Principles"	means the NCSC's document "Secure Design Principles", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cyber-security-design-principles.
"OWASP"	means the Open Web Application Security Project Foundation;
"OWASP Secure Coding Practice"	means the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at

	https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content;
"OWASP Top Ten"	means the list of the most critical security risks to web applications published annually by OWASP and found at https://owasp.org/www-project-top-ten/;
"Privileged User"	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
"Process"	means any operation performed on data (which includes without limitation, Personal Data), whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data, and "Processing" shall be interpreted accordingly";
"Prohibited Activity"	means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice;
"Prohibition Notice"	means a notice issued under paragraph 1.8 of the Security Requirements.
"Protective Monitoring System"	means the system implemented by the Supplier and its Sub-contractors under paragraph 12.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code
"Register of Support Locations and Third-Party Tools"	means the part of the Security Management Plan setting out, in respect of Support Locations and Third-Party Tools: (a) the nature of the activity performed at the Support Location or by the Third-Party Tool on the Code or the Buyer Data (as applicable); (b) where that activity is performed by individuals, the place or facility from where that activity is performed; and (c) in respect of the entity providing the Support Locations or Third-Party Tools, its: (i) full legal name; (ii) trading name (if any) (iii) country of registration; (iv) registration number (if applicable); and (v) registered address.
"Relevant Activities"	means those activities specified in paragraph 1.1 of the Security Requirements.
"Relevant Certifications"	means:

	(a) in the case of the Supplier, any SIMS Sub-contractor and any Sub-contractor that Processes Buyer Data: (i) ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2013; and (ii) Cyber Essentials Plus; and (b) for all other Sub-contractors means Cyber Essentials Plus;
"Relevant Convictions"	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences) or any other offences relevant to Services as the Buyer may specify
"Remediation Action Plan"	means the plan prepared by the Supplier in accordance with Paragraph 10.20 to 10.24, addressing the vulnerabilities and findings in a IT Health Check report
"Risk Management Approval Statement"	the statement issued by the Buyer under Paragraph 15.2 following the Buyer-led Assurance of the Supplier Information Management System;
"Secure Development Guidance"	means the Supplier's secure coding policy required under its ISO27001 Relevant Certification;
"Security Management Plan"	means the document prepared in accordance with the requirements of Paragraph 13 and in the format, and containing the information, specified in Annex 2.
"Security Requirements"	mean the security requirements in Annex 1 to this Security Schedule
"Security Requirements for Development"	means the security requirement Annex 2 to this Security Schedule
"Security Test"	means: (a) an Buyer Security Test; (b) an IT Health Check; or (c) a Supplier Security Test.

"Security Working Group"	means the Board established under Paragraph 8 or Call Off Special Schedule 8 (Call Off Contract Management), as applicable;
"SIMS Sub-contractor"	means a Sub-contractor designated by the Buyer that provides or operates the whole, or a substantial part, of the Supplier Information Management System;
"Sites"	means any premises (including the Buyer Premises, the Supplier's premises or third-party premises): (a) from, to or at which: (i) the Services are (or are to be) provided; or (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where: (i) any part of the Supplier System is situated; or (ii) any physical interface with the Buyer System takes place;
"SMP Sub-contractor"	means a Sub-contractor with significant market power, such that: (c) they will not contract other than on their own contractual terms; and (d) either: (i) there are no other substitutable suppliers of the particular services other than SMP Sub-contractors; or (ii) the Sub-contractor concerned has an effective monopoly on the provision of the Services.
"Statement of Information Risk Appetite"	means the statement provided by the Buyer under Paragraph 7.1 setting out the nature and level of risk that the Supplier accepts from the operation of the Supplier Information Management System.
"Sub-contractor"	as defined in Schedule 1 (Definitions) and includes, for the purposes of this Security Schedule , any individual or entity that: (a) forms part of the supply chain of the Supplier; and (b) has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Buyer Data;
"Sub-contractor Personnel"	means: (c) any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and

	(d) engaged in or likely to be engaged in: (i) the performance or management of the Services; (ii) or the provision of facilities or services that are necessary for the provision of the Services.
"Sub-contractors' Systems"	means the information and communications technology system used by a Sub-contractor in implementing and performing the Services, including: (a) the Software; (b) the Supplier Equipment; (c) configuration and management utilities; (d) calibration and testing tools; (e) and related cabling; but does not include the Buyer System;
"Supplier Information Management System"	means (a) the Supplier System; (b) the Sites; (c) any part of the Buyer System the Supplier or any Sub-contractor will use to Process Buyer Data, or provide the Services; and (d) the associated information management system, including all relevant: (i) organisational structure diagrams, (ii) controls, (iii) policies, (iv) practices, (v) procedures, (vi) processes; and (vii) resources;
"Supplier Personnel"	means Supplier Staff as defined in Schedule 1 (Definitions);
"Supplier System"	means the information and communications technology system used by the Supplier in performing the Services including software (but excluding the Authority System);
"Support Location"	means a place or facility where or from which individuals may access or Process the Code or the Buyer Data;

“Support Register”	means the register of all hardware and software used to provide the Services produced and maintained in accordance with paragraph 4 of the Security Requirements.
“Third-party Software Module”	means any module, library or framework that: (a) is not produced by the Supplier or a Sub-contractor as part of the Development Activity; and (b) either: (i) forms, or will form, part of the Code; or (ii) is, or will be, accessed by the Developed System during its operation.
“Third-party Tool”	means any activity conducted other than by the Supplier during which the Code or the Buyer Data is accessed, analysed or modified or some form of operation is performed on it;
“UKAS”	means the United Kingdom Accreditation Service;
"Wider Information Management System”	means (e) any: (i) information assets, (ii) IT systems, (iii) IT services; or Sites that: (f) the Supplier or any Sub-contractor will use to: (i) Process, or support the Processing of, Buyer Data; or (ii) provide, or support the provision of, the Services; or (g) any IT systems controlled or operated by the Supplier or any Sub-contractor that interface such; together with the associated information management system, including all relevant: (i) organisational structure diagrams, (ii) controls, (iii) policies, (iv) practices, (v) procedures, (vi) processes; and (vii) resources.

3 Introduction

3.1 This Security Schedule sets out:

(a) the Buyer's decision on where the Supplier may:

(i) store, access or process Buyer Data;

(ii) undertake the Development Activity;

(iii) host the Development Environment; and

(iv) locate Support Locations,

(in Paragraph 1)

(b) the principles of security that apply to this Contract (in Paragraph 4);

(c) the requirement to obtain a Risk Management Approval Statement (in Paragraphs 6 and 15;

(d) the annual confirmation of compliance to be provided by the Supplier (in Paragraph 7);

(e) the governance arrangements for security matters, where these are not otherwise specified in Call Off Special Schedule 8 (Call Off Contract Management) (in Paragraph 8);

(f) access to personnel (in Paragraph 9);

(g) obligations in relation to Sub-contractors (in Paragraph 10);

(h) the responsibility of the Buyer to determine the Supplier Information Management System that will be subject to Buyer-led Assurance (in Paragraph 11);

(i) the Certification Requirements (in Paragraph 12);

(j) the development, monitoring and updating of the Security Management Plan by the Supplier (in Paragraphs 13, 14 and 15);

(k) the granting by the Buyer of approval for the Supplier to commence:

(i) the provision of Services; and/or

(ii) Processing Buyer Data (in Paragraph 6);

(l) the management of changes to the Supplier Information Management System (in Paragraph 16); and

(m) the Buyer's additional remedies for breach of this Security Schedule), including:

(i) the requirement for Remediation Action Plans (in Paragraph 17);

(ii) the appointment of Independent Security Advisers (in Paragraph 18); and

(iii) the withholding of Charges by the Buyer (in Paragraph 19).

4 Principles of security

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

(a) the Buyer System;

(b) the Supplier System;

(c) the Sites;

(d) the Services; and

(e) the Supplier Information Management System.

4.2 The Parties shall share information and act in a co-operative manner at all times to further the principles of security in Paragraph 4.1.

5 Security requirements

5.1 The Supplier must, unless otherwise agreed in writing with the Buyer:

(a) comply with the Security Requirements; and

(b) subject to Paragraph 5.2, ensure that Sub-contractors comply with the Security Requirements.

5.2 Where a Sub-contractor is a SMP Sub-contractor, the Supplier shall:

(a) use best endeavours to ensure that the SMP Sub-contractor complies with the Security Requirements;

(b) document the differences between Security Requirements the obligations that the SMP Sub-contractor is prepared to accept in sufficient detail to allow the Buyer to form an informed view of the risks concerned;

(c) take such steps as the Buyer may require to mitigate those risks.

5.3 Where the Supplier or any Sub-contractor undertakes Development Activity the Supplier must (where applicable) comply, and ensure that any applicable Sub-contractor complies, with the Security Requirements for Development.

6 Buyer to proceed

6.1 Notwithstanding anything in this Contract, the Supplier may not:

(a) commence the provision of any Services; or

(b) Process any Buyer Data using the Supplier Information Management System,

unless:

(c) the Supplier has, and ensured that Sub-contractors have, obtained the Relevant Certifications under Paragraph 12;

(d) the Supplier has completed an IT Health Check in accordance with paragraph 10 of the Security Requirements; and

(e) the Buyer has provided a Risk Management Approval Statement under Paragraph 13.

7 Supplier confirmation

7.1 The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its Chief Executive Officer (or equivalent officer) confirming that, having made due and careful enquiry:

(a) the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Contract;

(b) subject to Paragraph 7.2:

(i) it has fully complied with all requirements of this Security Schedule ; and

(ii) all Sub-contractors have complied with the requirements of this Security Schedule with which the Supplier is required to ensure they comply;

(c) the Supplier considers that its security and risk mitigation procedures remain effective.

7.2 Where the Buyer has, in respect of the period covered by the confirmation provided under Paragraph 7.1 agreed in writing that the Supplier need not, or need only partially, comply within any requirement of this Security Schedule :

(a) the confirmation must include details of the Buyer's agreement; and

(b) confirm that the Supplier has fully complied with that modified requirement.

7.3 The Supplier must:

(a) keep and maintain a register setting out all agreements referred to in Paragraph 7.2; and

(b) provide a copy of that register to the Buyer on request.

8 Governance

8.1 This Paragraph 8 applies where a Security Working Group, or other board under this Call-Off Contract with a similar remit, is not provided for otherwise in this Contract.

8.2 The Buyer must establish a Security Working Group on which both the Buyer and the Supplier are represented.

8.3 The notice or other document establishing the Security Working Group must set out:

(a) the Buyer members;

(b) the Supplier members;

(c) the chairperson of the Security Working Group;

(d) the date of the first meeting;

(e) the frequency of meetings; and

(f) the location of meetings

8.4 The Security Working Group has oversight of all matters relating to the security of the Buyer Data and the Supplier Information Management System.

8.5 The Security Working Group meets:

(a) once every Contract Year following the review of the Security Management Plan by the Supplier under Paragraph 14 and before the Buyer has completed its review of the updated Security Management Plan under Paragraph 15; and

(b) additionally when required by the Buyer.

8.6 The Supplier must ensure that the Supplier Personnel attending each meeting of the Security Working Group:

(a) have sufficient knowledge and experience to contribute to the discussion of the matters on the agenda for the meeting;

(b) are authorised to make decisions that are binding on the Supplier in respect of those matters, including any decisions that require expenditure or investment by the Supplier; and

(c) where relevant to the matters on the agenda for the meeting, include representatives of relevant Sub-contractors.

8.7 Any decisions, recommendations or advice of the Security Working Group:

(a) are not binding on the Supplier; and

(b) do not limit or modify the Supplier's responsibilities under this Security Schedule

8.8 Appendix 3 applies to the Security Working Group.

9 Personnel

9.1 The Supplier must ensure that at all times it maintains within the Supplier Personnel sufficient numbers of qualified, skilled security professionals to ensure the Supplier complies with the requirements of this Security Schedule.

9.2 To facilitate:

(a) the Buyer's oversight of the Supplier Information Management System; and

(b) the Supplier's design, implementation, operation, management and continual improvement of the Security Management Plan and the security of the Services and Information Management System and otherwise,

at reasonable times and on reasonable notice:

(c) the Supplier shall provide access to the Supplier Personnel responsible for information assurance; and

(d) the Buyer shall provide access to its personnel responsible for information assurance.

10 Sub-contractors

SIMS Sub-contractor

10.1 Notwithstanding anything else in this Contract but subject to Paragraph , a SIMS Sub-contractor shall be treated for all purposes as a Key Sub-contractor.

10.2 In addition to the obligations imposed by this Contract on Key Sub-contractors, the Supplier must ensure that the Key Subcontract with each SIMS Sub-contractor:

(a) contains obligations no less onerous on the Key Sub-contractor than those imposed on the Supplier under this Security Schedule ; and

(b) provides for the Buyer to perform Buyer-led Assurance of any part of the Supplier Information Management System that the SIMS Sub-contractor provides or operates that is not otherwise subject to Buyer-led Assurance under this Security Schedule).

10.3 Where a SIMS Sub-contractor is also a SMP Sub-contractor, the Supplier shall:

(a) use best endeavours to ensure that the SMP Sub-contractor complies with the requirements of this Contract relating to Key Sub-contractors;

(b) document the differences between the Key Sub-contractor obligations imposed by this Contract and the Key Sub-contractor obligations that the SMP Sub-contractor is prepared to accept in sufficient detail to allow the Buyer to form an informed view of the risks concerned;

(c) take such steps as the Buyer may require to mitigate those risks.

Sub-contractors

10.4 Unless otherwise set out in the table in Appendix 4 (*Sub-contractor Security Requirements and Security Requirements for Development*), the Supplier must ensure that Sub-contractors comply with all Security Requirements and Security Requirements for Development that apply to the activities that the Sub-contractor performs under its Sub-contract with the Supplier.

10.5 The Supplier must, before entering into a binding Sub-contract with any Sub-contractor:

(a) undertake sufficient due diligence of the proposed Sub-contractor to provide reasonable assurance that the proposed Sub-contractor can perform the obligations that this Schedule requires the Supplier ensure that the proposed Sub-contractor performs;

(b) keeps adequate records of the due diligence it has undertaken in respect of the proposed Sub-contractors; and

(c) provides those records to the Buyer on request.

11 Supplier Information Management System

11.1 The Supplier must determine:

(a) the scope and component parts of the Supplier Information Management System; and

(b) the boundary between the Supplier Information Management System and the Wider Information Management System.

11.2 Before making the determination under Paragraph 11.1, the Supplier must consult with the Buyer and in doing so must provide the Buyer with such documentation and information that the Buyer may require regarding the Wider Information Management System.

11.3 The Supplier shall reproduce its determination under Paragraph 11.1 as a diagram documenting the components and systems forming part of the Information Management System and the boundary between the Supplier Information Management System and the Wider Information Management System.

11.4 The diagram prepared under Paragraph 11.3 forms part of the Security Management Plan.

11.5 Any proposed change to:

(a) the component parts of the Supplier Information Management System; or

(b) the boundary between the Supplier Information Management System and the Wider Information Management System,

is:

(a) an Operational Change to which the Change Control Procedure applies;

(b) requires approval by the Buyer under Paragraph 16; and

(c) the Buyer may require the appointment of an Independent Security Adviser to advise on the proposed change.

12 Certification Requirements

12.1 The Supplier shall ensure that, unless otherwise agreed by the Buyer, both:

(a) it; and

(b) any Sub-contractor,

are certified as compliant with the Relevant Certifications, that is to say:

(c) in the case of the Supplier, any SIMS Sub-contractor and any Sub-contractor that Processes Buyer Data:

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

(ii) Cyber Essentials Plus; and

(d) for all other Sub-contractors, Cyber Essentials Plus.

12.2 Unless otherwise agreed by the Buyer, before it begins to provide the Services, the Supplier must provide the Buyer with a copy of:

(a) the Relevant Certifications for it and any Sub-contractor; and

(b) the relevant scope and statement of applicability required under the ISO/IEC 27001:2013 Relevant Certifications.

12.3 The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications for it and any Sub-contractor are:

(a) currently in effect;

(b) cover at least the full scope of the Supplier Information Management System; and

(c) are not subject to any condition that may impact the provision of the Services or the Development Activity,

(the "**Certification Requirements**").

12.4 The Supplier must notify the Buyer promptly, and in any event within 3 Working Days, after becoming aware that, in respect of it or any Sub-contractor:

(a) a Relevant Certification has been revoked or cancelled by the body that awarded it;

(b) a Relevant Certification expired and has not been renewed by the Supplier;

(c) a Relevant Certification no longer applies to the full scope of the Supplier Information Management System; or

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

12.5 Where the Supplier has notified the Buyer of a Certification Default under Paragraph 12.4:

(a) the Supplier must, within 10 Working Days of the date in which the Supplier provided notice under Paragraph 12.4 (or such other period as the Parties may agree) provide a draft plan (a "**Certification Rectification Plan**") to the Buyer setting out:

(i) full details of the Certification Default, including a root cause analysis;

(ii) the actual and anticipated effects of the Certification Default;

(iii) the steps the Supplier and any Sub-contractor to which the Certification Default relates will take to remedy the Certification Default;

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

(c) if the Buyer rejects the Certification Rectification Plan, the Supplier must within 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph 12.5(b) will apply to the re-submitted plan;

(d) the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Contract;

(e) if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

13 Security Management Plan

Purpose of Security Management Plan

13.1 The Buyer may, at any time, provide the Supplier with a Statement of Risk Appetite.

13.2 The Supplier must document in the Security Management Plan how the Supplier and its Sub-contractors will:

(a) comply with the requirements set out in this Security Schedule and the Contract in order to ensure the security of the Buyer Data and the Supplier Information Management System; and

(b) ensure that the operation of the Supplier Information Management System and the provision of the Services does not give risk to any information security risks greater than those set out in that Statement of Information Risk Appetite (where one has been provided).

13.3 The Supplier must ensure that:

(a) the Security Management Plan accurately represents the Supplier Information Management System;

(b) the Supplier Information Management System will meet the requirements of this Security Schedule and the Statement of Risk Appetite (where one has been provided); and

(c) the residual risks of the Supplier Information Management System are no greater than those provided for in the Statement of Risk Appetite (where one has been provided).

Preparation of Security Management Plan

13.4 The Supplier must prepare and submit the Security Management Plan to the Buyer:

(a) by the date specified in the Detailed Implementation Plan; or

(b) if no such date is specified, in sufficient time to allow for the Buyer to review and approve the Security Management Plan before the first Operational Service Commencement Date.

13.5 If Paragraph 13.4(b) applies, and any delay resulting from the Buyer's review and approval of the Security Management Plan causes or contributes to Supplier Non-Performance under Clause 32.1, that delay is not a Buyer Cause and the Supplier shall not be entitled to any relief or compensation under Clause 32.

Contents of Security Management Plan

13.6 The Security Management Plan must use the template in Appendix 5 and must include:

(a) a formal risk assessment of, and a risk treatment plan for, the Supplier Information Management System;

(b) a completed ISO/IEC 27001:2013 statement of applicability for the Supplier Information Management System;

(c) the process for managing any security risks from Sub-contractors and third parties with access to the Services, the Supplier Information Management System or the Buyer Data;

(d) unless such requirement is waived by the Buyer, the controls the Supplier will implement in respect of the Services and all processes associated with the delivery of the Services, including:

(i) the Buyer Premises;

(ii) the Sites;

(iii) the Supplier System;

(iv) the Buyer System (to the extent that it is under the control of the Supplier); and

(v) any IT, Information and data (including the Confidential Information of the Buyer and the Buyer Data) to the extent used by the Buyer or the Supplier:

(A) in connection with this Contract or

(B) in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

(e) evidence that the Supplier and each applicable Sub-contractor is compliant with the Certification Requirements; and

(f) the diagram documenting the Supplier Information Management System, the Wider Information Management System and the boundary between them (created under Paragraph 11).

(g) an assessment of the Supplier Information Management System against the requirements of this Security Schedule , including the Security Requirements and the Security Requirements for Development (where applicable);

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

(i) the following information, so far as is applicable, in respect of each Sub-contractor:

(i) the Sub-contractor's:

(A) legal name;

(B) trading name (if any); and

(C) registration details (where the Sub-contractor is not an individual);

(ii) the Relevant Certifications held by the Sub-contractor;

(iii) the Sites used by the Sub-contractor;

(iv) the Services provided, or contributed to, by the Sub-contractor;

(v) the access the Sub-contractor has to the Supplier Information Management System;

(vi) the Buyer Data Processed by the Sub-contractor;

(vii) the Processing that the Sub-contractor will undertake in respect of the Buyer Data; and

(viii) the measures the Sub-contractor has in place to comply with the requirements of this Security Schedule);

(j) the Register of Support Locations and Third Party Tools;

(k) the Modules Register;

(l) the Support Register; and

(m) details of the protective monitoring that the Supplier will undertake in accordance with paragraph 12 of the Security Requirements, including:

(i) the additional audit and monitoring the Supplier will undertake of the Supplier Information Management System; and

(ii) the retention periods for audit records and event logs.

14 Monitoring and updating Security Management Plan

Updating Security Management Plan

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

Monitoring

14.2 The Supplier, where it plans to undertake, or after becoming aware of, any of the following:

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

(b) a significant change in the boundary between the Supplier Information Management System and the Wider Information Management System;

(c) a significant change in the operation of the Supplier Information Management System;

(d) the replacement of an existing, or the appointment of a new:

(i) SIMS Sub-contractor; or

(ii) Sub-contractor that Processes Buyer Data;

(e) a significant change in the quantity of Personal Data held within the Service; and/or

(f) where the Supplier has previously Processed Buyer Data that is Personal Data, not including Special Category Personal Data, it proposes to start to Process Buyer Data that is Special Category Personal Data under this Contract;

must:

(g) within 2 Working Days notify the Buyer; and

(h) within 10 Working Days, or such other timescale as may be agreed with the Buyer, update the Security Management Plan and provide the Buyer with a copy that document for review and approval.

14.3 Paragraph 14.2 applies in addition to, and not in substitution of, the Parties' obligations to comply with the Change Control Procedure for any Contract Change or Operational Change.

14.4 Any proposed change under Paragraph 14.2(a), 14.2(b) or 14.2(f) is a Contract Change to which the Change Control Procedure applies.

15 Review and approval of Security Management Plan

15.1 Where the Supplier has prepared or updated the Security Management Plan the Buyer may review the plan and to do so may request such further information as the Buyer considers necessary or desirable.

15.2 At the conclusion of that review, it may issue to the Supplier:

(a) where satisfied that the:

(i) identified risks to the Supplier Information Management System are adequately and appropriately addressed; and

(ii) that the residual risks are:

(A) either:

(1) where the Buyer has provided a Statement of Information Risk Appetite, reduced to the level anticipated by that statement; or

(2) where the Buyer has not provided a Statement of Information Risk Appetite, reduced to an acceptable level;

(B) understood and accepted by the Buyer; and

(C) recorded in the Residual Risk Statement;

a Risk Management Approval Statement; or

(b) where the Buyer considers that:

(i) the identified risks to the Supplier Information Management System have not been adequately or appropriately addressed; or

(ii) the residual risks to the Supplier Information Management System have not been reduced:

(A) where the Buyer has Provided a Statement of Information Risk Appetite, to the level anticipated by that statement; or

(B) where the Buyer has not Provided a Statement of Information Risk Appetite, to an acceptable level,

a Risk Management Rejection Notice, with the reasons for its decision.

16 Changes to the Supplier Information Management System

16.1 Notwithstanding anything in this Contract, the Supplier must obtain the approval of the Buyer before making **any of the following changes to the Supplier Information Management System:**

(a) **a significant change in the systems or components making up the Supplier Information Management System;**

(b) **a significant change in the operation or management of the Supplier Information Management System; or**

(c) **the appointment of a new, or the replacement of an existing:**

(i) **SIMS Sub-contractor; or**

(ii) **Sub-contractor that Processes Buyer Data.**

16.2 In seeking the Buyer's approval to a proposed changes to the Supplier Information Management System, the Supplier must:

(a) prepare a proposal for the Buyer setting out:

(i) details of the proposed changes to the Supplier Information Management System;

(ii) an assessment of the security implications of the proposed change;

(iii) a risk assessment of the proposed change;

(b) provide that paper to the Buyer no later than 30 Working Days before the date on which the Supplier proposes to implement those changes.

16.3 The Buyer:

(a) may request such further information as the Buyer considers necessary or desirable;

(b) must provide its decision within 20 Working Days of the later of:

(i) the date on which it receives the proposal; or

(ii) the date on which it receives any requested further information;

(c) must not:

(i) unreasonably refuse any proposal by the Supplier; and

(ii) must not make any approval subject to unreasonable conditions.

16.4 If the Buyer does not provide a decision within the period specified in Paragraph 16.3(b), the proposal shall be deemed to have been accepted.

Implementation of changes

16.5 Where the Supplier implements a necessary change to the Supplier Information Management System to address a security related risk or vulnerability, the Supplier shall effect such change at its own cost and expense.

16.6 If the Supplier does not implement a necessary change to the Supplier Information Management System to address a security related risk or vulnerability:

(a) that failure is a material Default; and

(b) the Supplier shall:

(i) immediately cease using the Supplier Information Management System to Process Buyer Data either:

(A) until the Default is remedied, or

(B) unless directed otherwise by the Buyer in writing and then only in accordance with the Buyer's written directions; and

(ii) where such material Default is capable of remedy, remedy such material Default within the timescales set by the Buyer (considering the security risks the material Default presents to the Services and/or the Supplier Information Management System).

17 Remediation Action Plan

Preparation of Remediation Action Plan

17.1 Where:

(a) the Buyer issues a Risk Management Rejection Notice; or

(b) the Supplier receives a Security Test report identifies vulnerabilities in, or makes findings in respect of, the Supplier Information Management System,

the Supplier must within 20 Working Days of receiving the notice or report, as applicable, prepare a plan addressing the matters raised in the notice or report, as applicable (a "**Remediation Action Plan**").

17.2 The Remediation Action Plan must, in respect of each matter raised by Risk Management Rejection notice or the Security Test report:

(a) how the matter will be remedied;

(b) the date by which the matter will be remedied; and

(c) the tests that the Supplier proposes to perform to confirm that the matter has been remedied.

Consideration of Remediation Action Plan

17.3 The Supplier must

(a) provide the Buyer with a copy of any Remediation Action Plan it prepares; and

(b) have regarded to any comments the Buyer provides in the Remediation Action Plan.

Implementing an approved Remediation Action Plan

17.4 In implementing the Remediation Action Plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.

17.5 If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within 2 Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:

(a) provide the Buyer with a full, unedited and unredacted copy of the test report;

(b) implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;

(c) as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

18 Independent Security Adviser

18.1 The Buyer may require the appointment of an Independent Security Adviser where:

(a) there is a proposed change to the Supplier Information Management System (see Paragraph 11.5);

(b) the Buyer issues two or more Risk Management Rejection Notices (see Paragraph 15.2(b)); or

(c) a Security Test (see paragraph 10 of the Security Requirements) report identifies more than 10 vulnerabilities classified as either critical or high; or

18.2 Where the Buyer requires the appointment of an Independent Security Adviser the Independent Security Adviser shall be:

(a) a person selected by the Supplier and approved by the Buyer; or

(b) where

(i) the Buyer does not approve the persons selected by the Supplier; or

(ii) the Supplier does not select any person within 10 Working Days of the date of the notice requiring the Independent Security Adviser's appointment,

a person selected by the Buyer.

18.3 The terms of the Independent Security Adviser's appointment shall require that person to:

(a) undertake a detailed review, including a full root cause analysis where the Independent Security Adviser considers it appropriate to do so, of the circumstances that led to that person's appointment; and

(b) provide advice and recommendations on:

(i) steps the Supplier can reasonably take to improvement the security of the Supplier Information Management System; and

(ii) where relevant, how the Supplier may mitigate the effects of, and remedy, those and to avoid the occurrence of similar circumstances to those leading to the appointment of the Independent Security Adviser in the future.

18.4 The Supplier must permit, and must ensure that relevant Sub-contractors permit, the Independent Security Adviser to:

(a) observe the conduct of and work alongside the Supplier Personnel to the extent that the Independent Security Adviser considers reasonable and proportionate having regard to reason for their appointment;

(b) gather any information the Independent Security Adviser considers relevant in the furtherance their appointment;

(c) write reports and provide information to the Buyer in connection with the steps being taken by the Supplier to remedy the matters leading to the Independent Security Adviser's appointment;

(d) make recommendations to the Buyer and/or the Supplier as to how the matters leading to their appointment might be mitigated or avoided in the future; and/or

(e) take any other steps that the Buyer and/or the Independent Security Adviser reasonably considers necessary or expedient in order to mitigate or rectify matters leading to the Independent Security Adviser's appointment.

18.5 The Supplier must, and ensure that relevant Sub-contractors:

(a) where relevant, work alongside, provide information to, co-operate in good faith with and adopt any reasonable methodology in providing the Services recommended by the Independent Security Adviser in order to mitigate or rectify any of the vulnerabilities that led to the appointment of the Independent Security Adviser;

(b) ensure that the Independent Security Adviser has all the access it may require in order to carry out its objective, including access to the Assets;

(c) submit to such monitoring as the Buyer and/or the Independent Security Adviser considers reasonable and proportionate in respect of the matters giving rise to their appointment;

(d) implement any recommendations (including additional security measures and/or controls) made by the Independent Security Adviser that have been approved by the Buyer within the timescales given by the Independent Security Adviser; and

(e) not terminate the appointment of the Independent Security Adviser without the prior consent of the Buyer (unless such consent has been unreasonably withheld).

18.6 The Supplier shall be responsible for:

(a) the costs of appointing, and the fees charged by, the Independent Security Adviser; and

(b) its own costs in connection with any action required by the Buyer and/or the Independent Security Adviser.

If the Supplier or any relevant Sub-contractor:

(c) fails to perform any of the steps required by the Buyer in the notice appointing the Independent Security Adviser; and/or

(d) is in Default of any of its obligations under this Paragraph 18,

this is a material Default that is capable of remedy.

19 Withholding of Charges

19.1 The Buyer may withhold some or all of the Charges in accordance with the provisions of this Paragraph 19 where:

(a) the Supplier is in material Default of any of its obligations under this Security Schedule ; or

(b) any of the following matters occurs (where those matters arise from a Default by the Supplier of its obligations under this Security Schedule):

(i) the Buyer is entitled to terminate the Contract for material Default on any of the grounds set out in Clause 35.2.1 (a) to (e) inclusive; or

(ii) the Supplier commits a material Default that is capable of remedy and the Buyer is entitled to step-in pursuant to Clause 31.13(b) or (c).

19.2 The Buyer may withhold an amount of the Charges that it considers sufficient, in its sole discretion, to incentivise the Supplier to perform the obligations it has Defaulted upon.

Before withholding any Charges under Paragraph 19.1 the Buyer must

(a) provide written notice to the Supplier setting out:

(i) the Default in respect of which the Buyer has decided to withhold some or all of the Charges;

(ii) the amount of the Charges that the Buyer will withhold;

(iii) the steps the Supplier must take to remedy the Default;

(iv) the date by which the Supplier must remedy the Default;

(v) the invoice in respect of which the Buyer will withhold the Charges; and

(b) consider any representations that the Supplier may make concerning the Buyer's decision.

19.3 Where the Supplier does not remedy the Default by the date specified in the notice given under Paragraph 19.3(a), the Buyer may retain the withheld amount.

The Supplier acknowledges:

(a) the legitimate interest that the Buyer has in ensuring the security of the Supplier Information Management System and the Buyer Data and, as a consequence, the performance by the Supplier of its obligations under this Security Schedule ; and

(b) that any Charges that are retained by the Buyer are not out of all proportion to the Buyer's legitimate interest, even where:

(i) the Buyer has not suffered any Losses as a result of the Supplier's Default; or

(ii) the value of the Losses suffered by the Buyer as a result of the Supplier's Default is lower than the amount of the Charges retained

19.4 The Buyer's right to withhold or retain any amount under this Paragraph 19 are in addition to any other rights that the Buyer may have under this Contract or in Law, including any right to claim damages for Losses it suffers arising from the Default.

20 Access to Buyer System

Where the Supplier, a Sub-contractor or any of the Supplier Personnel is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such

Sub-contractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

Appendix 1 Security Requirements

1. Location

Location for Relevant Activities

1.1 Unless otherwise agreed with the Buyer, the Supplier must, and ensure that its Sub-contractors, at all times:

(a) store, access or process Buyer Data;

(b) undertake the Development Activity; and

(c) host the Development Environment,

(together, the "**Relevant Activities**")

only in or from the geographic areas permitted by the Buyer in Paragraph 1.

1.2 Where the Buyer has permitted the Supplier and its Sub-contractors to perform the Relevant Activities outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors undertake the Relevant Activities in a facility operated by an entity where:

(a) the entity has entered into a binding Contract with the Supplier or Sub-contractor (as applicable);

(b) that binding Contract includes obligations on the entity in relation to security management equivalent to those imposed on Sub-contractors in this Security Schedule ;

(c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding Contract;

(d) the Supplier has provided the Buyer with such information as the Buyer requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

(iii) the entity's compliance with the binding Contract; and

(e) the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.8.

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

(a) it must provide the Buyer with such information as the Buyer requests concerning:

(i) the security controls in places at the relevant location or locations; and

(ii) where certain security controls are not, or only partially, implemented the reasons for this;

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

(c) if the Buyer does not grant permission to use that location or those locations, the Supplier must, within such period as the Buyer may specify:

(i) cease to store, access or process Buyer Data at that location or those locations;

(ii) sanitise, in accordance with instructions from the Buyer, such equipment within the information and communications technology system used to store, access or process Buyer Data at that location, or those locations, as the Buyer may specify.

Support Locations

1.4 The Supplier must ensure that all Support Locations are located only in the geographic areas permitted by the Buyer.

1.5 Where the Buyer has permitted the Supplier and its Sub-contractors to operate Support Locations outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors operate the Support Locations in a facility operated by an entity where

(a) the entity has entered into a binding Contract with the Supplier or Sub-contractor (as applicable);

(b) the binding Contract includes obligations in relations to security management at least as onerous as those imposed on any Sub-contractor by this Security Schedule ;

(c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding Contract;

(d) the Supplier has provided the Buyer with such information as the Buyer requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

(iii) the entity's compliance with the binding Contract; and

(iv) the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.8.

Third-party Tools

1.6 The Supplier must use, and ensure that Sub-contractors use, only those Third-party Tools included in the Register of Support Locations and Third-party Tools.

1.7 The Supplier must not, and must not allow Sub-contractors to, use:

1.7.1 a Third-party Tool other than for the activity specified for that Third-party Tool in the Register of Support Locations and Third-party Tools; or

1.7.2 a new Third-party Tool, or replace an existing Third-party Tool, without the permission of the Buyer.

Prohibited Activities

1.8 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken some or all of the Relevant Activities or operate Support Locations (a "**Prohibited Activity**").

1.8.1 in any particular country or group of countries;

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

1.8.3 in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity,

(a "**Prohibition Notice**").

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

1.10 Nothing in this Paragraph 1 shall affect the Parties obligations to comply with Clause 34.7.4 and the conditions set out therein shall continue to apply in addition to the requirements of this Paragraph 1.

2. Vetting, Training and Staff Access

Vetting before performing or managing Services

2.1 The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel in:

2.1.1 Development Activity;

2.1.2 any activity that provides access to the Development Environment; or

2.1.3 any activity relating to the performance and management of the Services

unless:

2.1.4 that individual has passed the security checks listed in paragraph 2.2; or

2.1.5 the Buyer has given prior written permission for a named individual to perform a specific role.

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

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

2.2.1.1 the individual's identity;

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

2.2.1.3 the individual's previous employment history; and

2.2.1.4 that the individual has no Relevant Convictions;

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

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

Annual training

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

2.3.1 General training concerning security and data handling; and

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

Staff access

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

2.5 The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.

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

Exception for certain Sub-contractors

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

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

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

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

3. End-user Devices

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

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

3.1.2 users must authenticate before gaining access;

3.1.3 all Buyer Data and Code must be encrypted using a encryption tool agreed to by the Buyer;

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

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

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

3.1.7 all End-user Devices are within the scope of any Relevant Certification.

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

3.3 Where there any conflict between the requirements of this Security Schedule and the requirements of the NCSC Device Guidance, the requirements of this Schedule take precedence.

4. Hardware and software support

4.1 The Supplier must ensure that all software used to provide the Services remains at all times in full security support, including any extended or bespoke security support.

4.2 The Supplier must produce and maintain a register of all software that form the Supplier Information Management System (the "**Support Register**").

4.3 The Support Register must include in respect of each item of software:

4.3.1 the date, so far as it is known, that the item will cease to be in mainstream security support; and

4.3.2 the Supplier's plans to upgrade the item before it ceases to be in mainstream security support.

4.4 The Supplier must:

4.4.1 review and update the Support Register:

4.4.1.1 within 10 Working Days of becoming aware of the date on which, or any change to the date on which, any item of software will cease to be in mainstream security report;

4.4.1.2 within 10 Working Days of introducing new software, or removing existing software, from the Supplier Information Management System; and

4.4.1.3 at least once every 12 months;

4.4.2 provide the Buyer with a copy of the Support Register:

4.4.2.1 whenever it updates the Support Register; and

4.4.2.2 otherwise when the Buyer requests.

4.5 Where any element of the Developed System consists of COTS Software, the Supplier shall ensure:

4.5.1 those elements are always in mainstream or extended security support from the relevant vendor; and

4.5.2 the COTS Software is not more than one version or major release behind the latest version of the software.

4.6 The Supplier shall ensure that all hardware used to provide the Services, whether used by the Supplier or any Sub-contractor is, at all times, remains in mainstream vendor support, that is, that in respect of the hardware, the vendor continues to provide:

4.6.1 regular firmware updates to the hardware; and

4.6.2 a physical repair or replacement service for the hardware.

5. Encryption

5.1 Before Processing any Buyer Data, the Supplier must agree with the Buyer the encryption methods that it and any Sub-contractors that Process Buyer Data will use to comply with this paragraph 5.

5.2 Where this paragraph 5 requires Buyer Data to be encrypted, the Supplier must use, and ensure that Subcontractors use, the methods agreed by the Buyer under paragraph 5.1.

5.3 Notwithstanding anything in the specification for the Developed System or this Contract, the Supplier must ensure that the Developed System encrypts Buyer Data:

5.3.1 when the Buyer Data is stored at any time when no operation is being performed on it; and

5.3.2 when the Buyer Data is transmitted.

5.4 Unless paragraph 5.5 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer Data is encrypted:

5.4.1 when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and

5.4.2 when transmitted.

5.5 Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 5.4, the Supplier must:

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

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

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

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

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

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

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

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

6. Email

6.1 Notwithstanding anything in the specification for the Developed System or this Contract, the Supplier must ensure that where the Developed System will provide an Email Service to the Buyer, the Developed System:

6.1.1 supports transport layer security ("**TLS**") version 1.2, or higher, for sending and receiving emails;

6.1.2 supports TLS Reporting ("**TLS-RPT**");

6.1.3 is capable of implementing:

6.1.3.1 domain-based message authentication, reporting and conformance ("**DMARC**");

6.1.3.2 sender policy framework ("**SPF**"); and

6.1.3.3 domain keys identified mail ("**DKIM**"); and

6.1.4 is capable of complying in all respects with any guidance concerning email security as issued or updated from time to time by:

6.1.4.1 the UK Government (current version at https://www.gov.uk/guidance/set-up-government-email-services-securely; or

6.1.4.2 the NCSC (current version at https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing).

7. DNS

Unless otherwise agreed by the Buyer, the Supplier must ensure that the Developed System uses the UK public sector Protective DNS ("**PDNS**") service to resolve internet DNS queries.

8. Malicious Software

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

8.2 The Supplier must ensure that such Anti-virus Software:

8.2.1 prevents the installation of the most common forms of Malicious Software in the Supplier Information Management System and the Development Environment;

8.2.2 is configured to perform automatic software and definition updates;

8.2.3 provides for all updates to be the Anti-virus Software to be deployed within 10 Working Days of the update's release by the vendor;

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

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

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

8.4 The Supplier must at all times, during and after the Term (up to the statutory limitation period of 6 + 1 year after contract), on written demand indemnify the Buyer and keep the Buyer indemnified, against all Losses incurred by, awarded against or agreed to be paid by the Buyer arising from any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Supplier, or a Sub-contractor, to comply with this paragraph .

9. Vulnerabilities

9.1 Unless the Buyer otherwise agrees, the Supplier must ensure that it or any relevant Sub-contractor applies security patches to any vulnerabilities in the Supplier Information Management System no later than:

9.1.1 7 days after the public release of patches for vulnerabilities classified as "critical";

9.1.2 30 days after the public release of patches for vulnerabilities classified as "important"; and

9.1.3 60 days after the public release of patches for vulnerabilities classified as "other".

9.2 The Supplier must:

9.2.1 scan the Supplier Information Management System and the Development Environment at least once every month to identify any unpatched vulnerabilities; and

9.2.2 if the scan identifies any unpatched vulnerabilities ensure they are patched in accordance with paragraph 9.1.

9.3 For the purposes of this paragraph 9, the Supplier must implement a method for classifying vulnerabilities to the Supplier Information Management System as "critical", "important" or "other" that is aligned to recognised vulnerability assessment systems, such as:

9.3.1.1 the National Vulnerability Database's vulnerability security ratings; or

9.3.1.2 Microsoft's security bulletin severity rating system.

10. Security testing

Responsibility for security testing

10.1 The Supplier is solely responsible for:

(a) the costs of conducting any security testing required by this paragraph 10 (unless the Buyer gives notice under paragraph 10.2); and

(b) the costs of implementing any findings, or remedying any vulnerabilities, identified in that security testing.

Security tests by Buyer

10.2 The Buyer may, where it has significant concerns relating to the security of the Supplier Information Management System, give notice to the Supplier that the Buyer will undertake the Supplier Security Tests.

10.3 Where the Buyer gives notice under paragraph 10.2:

(a) the Supplier shall provide such reasonable co-operation as the Buyer requests, including:

(i) such access to the Supplier Information Management System as the Buyer may request; and

(ii) such technical and other information relating to the Information Management System as the Buyer requests;

(b) the Buyer must provide a full, unedited and unredacted copy of the report relating to the IT Health Check as soon as reasonably practicable after the Buyer receives a copy of the report; and

(c) for the purposes of paragraphs 10.18 to 10.27:

(i) the Supplier must treat any IT Health Check commissioned by the Buyer as if it were such a report commissioned by the Supplier; and

(ii) the time limits in paragraphs 10.18 and 10.20 run from the date on which the Buyer provides the Supplier with the copy of the report under paragraph (b).

10.4 In addition to its rights under paragraph 10.2, the Buyer and/or its authorised representatives may, at any time and without giving notice to the Supplier, carry out such tests (including penetration tests) as it may deem necessary in relation to:

(a) the Service;

(b) the Supplier Information Management System; and/or

(c) the Supplier's compliance with the Security Management Plan,

(“**Buyer Security Tests**”).

10.5 The Buyer shall take reasonable steps to notify the Supplier prior to carrying out such Buyer Security Tests to the extent that it is reasonably practicable for it to do so taking into account the nature of the Buyer Security Tests.

10.6 The Buyer shall notify the Supplier of the results of such Buyer Security Tests after completion of each Buyer Security Test.

10.7 The Buyer shall design and implement the Buyer Security Tests to minimise their impact on the delivery of the Services.

10.8 If an Buyer Security Tests causes Supplier Non-Performance, the Buyer Security Tests shall be treated as an Buyer Cause, except where the root cause of the Supplier Non-Performance was a security-related weakness or vulnerability exposed by the Buyer Security Tests.

Security tests by Supplier

10.9 The Supplier must:

(a) before submitting the draft Security Management Plan to the Buyer for an Assurance Decision;

(b) at least once during each Contract Year; and

(c) when required to do so by the Buyer;

undertake the following activities:

(d) conduct security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment (an "**IT Health Check**") in accordance with paragraphs 10.15 to 10.17; and

(e) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with paragraphs 10.18 to 10.27.

10.10 In addition to its obligations under paragraph 10.9, the Supplier must undertake any tests required by:

(a) any Remediation Action Plan;

(b) the ISO27001 Certification Requirements;

(c) the Security Management Plan; and

(d) the Buyer, following a Breach of Security or a significant change, as assessed by the Buyer, to the components or architecture of the Supplier Information Management System,

(each a "**Supplier Security Test**").

10.11 The Supplier must

(a) design and implement the Supplier Security Tests so as to minimise the impact on the delivery of the Services;

(b) agree the date, timing, content and conduct of such Supplier Security Tests in advance with the Buyer.

10.12 Where the Supplier fully complies with paragraph 10.11, if a Supplier Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be entitled to relief in respect of such Performance Failure for that Measurement Period.

10.13 The Buyer may send a representative to witness the conduct of the Supplier Security Tests.

10.14 The Supplier shall provide the Buyer with a full, unedited and unredacted copy of the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable, and in any case within 10 Working Days, after completion of each Supplier Security Test

IT Health Checks

10.15 In arranging an IT Health Check, the Supplier must:

(a) use only a CHECK Service Provider to perform the IT Health Check;

(b) design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier Information Management System and the delivery of the Services.

(c) promptly provide the Buyer with such technical and other information relating to the Supplier Information Management System as the Buyer requests;

(d) include within the scope of the IT Health Check such tests as the Buyer requires;

(e) agree with the Buyer the scope, aim and timing of the IT Health Check.

10.16 The Supplier must commission the IT Health Check in accordance with the scope, aim and timing agreed by the Buyer.

10.17 Following completion of an IT Health Check, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the report relating to the IT Health Check without delay and in any event within 10 Working Days of its receipt by the Supplier.

Remedying vulnerabilities

10.18 In addition to complying with Paragraphs 10.20 to 10.27, the Supplier must remedy:

(a) any vulnerabilities classified as critical in a Security Test report within 5 Working Days of becoming aware of the vulnerability and its classification;

(b) any vulnerabilities classified as high in a Security Test report within 1 month of becoming aware of the vulnerability and its classification; and

(c) any vulnerabilities classified as medium in a Security Test report within 3 months of becoming aware of the vulnerability and its classification.

10.19 The Supplier must notify the Buyer immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as critical, high or medium in a Security Test report within the time periods specified in Paragraph 10.18.

Responding to a Security Test report

10.20 Where the Security Test report identifies vulnerabilities in, or makes findings in respect of, the Supplier Information Management System, the Supplier must within 20 Working Days of receiving the Security Test report, prepare and submit for approval to the Buyer a draft plan addressing the vulnerabilities and findings (the "**Remediation Action Plan**").

10.21 Where the Buyer has commissioned a root cause analysis under Paragraph 10.28, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.

10.22 The draft Remediation Action Plan must, in respect of each vulnerability identified or finding made by the Security Test report:

(a) how the vulnerability or finding will be remedied;

(b) the date by which the vulnerability or finding will be remedied; and

(c) the tests that the Supplier proposes to perform to confirm that the vulnerability has been remedied or the finding addressed.

10.23 The Supplier shall promptly provide the Buyer with such technical and other information relating to the Supplier Information Management System, the IT Health Check report or the draft Remediation Action Plan as the Buyer requests.

10.24 The Buyer may:

(a) reject the draft Remediation Action Plan where it considers that the draft Remediation Action Plan is inadequate, providing its reasons for doing so, in which case:

(i) the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Buyer's reasons; and

(ii) paragraph 10.22 to 10.24 shall apply, with appropriate modifications, to the revised draft Remediation Action Plan;

(b) accept the draft Remediation Action Plan, in which case the Supplier must immediately start work on implementing the Remediation Action Plan in accordance with Paragraph 10.26 and 10.27.

10.25 Where the Buyer unreasonably:

(a) delays its approval; or

(b) rejects,

the draft Remediation Action Plan, the Supplier will not be in breach of this Contract to the extent it demonstrates that any breach:

(c) arose directly from the Buyer unreasonably withholding or delaying, as appropriate, its approval of the draft Remediation Action Plan; and

(d) would not have occurred had:

(i) the Buyer given its approval, or given its approval in a timely manner, to the draft Remediation Action Plan; and

(ii) the Supplier had implemented the draft Remediation Action Plan in accordance with its terms.

Implementing an approved Remediation Action Plan

10.26 In implementing the Remediation Action Plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.

10.27 If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within [2] Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:

(a) provide the Buyer with a full, unedited and unredacted copy of the test report;

(b) implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;

(c) as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

Significant vulnerabilities

10.28 Where:

(a) a Security Test report identifies more than 10 vulnerabilities classified as either critical or high; or

(b) the Buyer rejected a revised draft Remediation Action Plan,

the Buyer may, at the Supplier's cost, either:

(c) appoint an independent and appropriately qualified and experienced security architect and adviser to perform a root cause analysis of the identified vulnerabilities; or

(d) give notice to the Supplier requiring the appointment as soon as reasonably practicable, and in any event within 10 Working Days, of an Independent Security Adviser.

11. Access Control

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

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

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

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

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

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

11.2.1 are allocated to a single, individual user;

11.2.2 are accessible only from dedicated End-user Devices;

11.2.3 are configured so that those accounts can only be used for system administration tasks;

11.2.4 require passwords with high complexity that are changed regularly;

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

11.2.6 are:

11.2.6.1 restricted to a single role or small number of roles;

11.2.6.2 time limited; and

11.2.6.3 restrict the Privileged User's access to the internet.

11.3 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that it logs all activity of the Privileged Users while those users access those accounts and keeps the activity logs for 20 Working Days before deletion.

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

11.5 The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in paragraphs 11.1 to 11.4.

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

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

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

12. Event logging and protective monitoring

Protective Monitoring System

12.1 The Supplier must, and must ensure that Sub-contractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code to:

12.1.1 identify and prevent potential Breaches of Security;

12.1.2 respond effectively and in a timely manner to Breaches of Security that do occur;

12.1.3 identify and implement changes to the Supplier Information Management System to prevent future Breaches of Security; and

12.1.4 help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier Information Management System or the Developed System

(the "**Protective Monitoring System**").

12.2 The Protective Monitoring System must provide for:

12.2.1 event logs and audit records of access to the Supplier Information Management system; and

12.2.2 regular reports and alerts to identify:

12.2.2.1 changing access trends;

12.2.2.2 unusual usage patterns; or

12.2.2.3 the access of greater than usual volumes of Buyer Data;

12.2.3 the detection and prevention of any attack on the Supplier Information Management System or the Development Environment using common cyber-attack techniques;

12.2.4 any other matters required by the Security Management Plan.

Event logs

12.3 The Supplier must ensure that, unless the Buyer otherwise agrees, any event logs do not log:

12.3.1 personal data, other than identifiers relating to users; or

12.3.2 sensitive data, such as credentials or security keys.

Provision of information to Buyer

12.4 The Supplier must provide the Buyer on request with:

12.4.1 full details of the Protective Monitoring System it has implemented; and

12.4.2 copies of monitoring logs and reports prepared as part of the Protective Monitoring System.

Changes to Protective Monitoring System

12.5 The Buyer may at any time require the Supplier to update the Protective Monitoring System to:

12.5.1 respond to a specific threat identified by the Buyer;

12.5.2 implement additional audit and monitoring requirements; and

12.5.3 stream any specified event logs to the Buyer's security information and event management system.

13. Audit rights

Right of audit

13.1 The Buyer may undertake an audit of the Supplier or any Sub-contractor to:

13.1.1 verify the Supplier's or Sub-contractor's (as applicable) compliance with the requirements of this Security Schedule and the Data Protection Legislation as they apply to Buyer Data;

13.1.2 inspect the Supplier Information Management System (or any part of it);

13.1.3 review the integrity, confidentiality and security of the Buyer Data; and/or

13.1.4 review the integrity and security of the Code.

13.2 Any audit undertaken under this Paragraph 13.1:

13.2.1 may only take place during the Term and for a period of 18 months afterwards; and

13.2.2 is in addition to and without prejudice to any other rights of audit the Buyer has under this Contract (including but not limited to, Clause 29).

13.3 The Buyer may not undertake more than one audit under Paragraph 13.1 in each calendar year unless the Buyer has reasonable grounds for believing:

13.3.1 the Supplier or any Sub-contractor has not complied with its obligations under this Contract or the Data Protection Legislation as they apply to the Buyer Data;

13.3.2 there has been or is likely to be a Breach of Security affecting the Buyer Data or the Code; or

13.3.3 where vulnerabilities, or potential vulnerabilities, in the Code have been identified by:

13.3.3.1 an IT Health Check; or

13.3.3.2 a Breach of Security.

Conduct of audits

13.4 The Buyer must use reasonable endeavours to provide 15 Working Days' notice of an audit.

13.5 The Buyer must when conducting an audit:

13.5.1 comply with all relevant policies and guidelines of the Supplier or Sub-contractor (as applicable) concerning access to the Suppler Information Management System the Buyer considers reasonable having regard to the purpose of the audit; and

13.5.2 use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the Supplier or Sub-contractor (as applicable) or delay the provision of the Services.

13.6 The Supplier must, and must ensure that Sub-contractors, on demand provide the Buyer with all co-operation and assistance the Buyer may reasonably require, including:

13.6.1 all information requested by the Buyer within the scope of the audit;

13.6.2 access to the Supplier Information Management System; and

13.6.3 access to the Supplier Personnel.

Response to audit findings

13.7 Where an audit finds that:

13.7.1 the Supplier or a Sub-contractor has not complied with this Contract or the Data Protection Legislation as they apply to the Buyer Data; or

13.7.2 there has been or is likely to be a Breach of Security affecting the Buyer Data

the Buyer may require the Supplier to remedy those defaults at its own cost and expense and within the time reasonably specified by the Buyer.

13.8 The exercise by the Buyer of any rights it may have under this Paragraph 3 does not affect the exercise by it of any other or equivalent rights it may have under this Contract in respect of the audit findings.

14. Breach of Security

Reporting Breach of Security

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

Immediate steps

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

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

14.2.2 remedy such Breach of Security to the extent possible;

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

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

Subsequent action

14.3 As soon as reasonably practicable and, in any event, within 5 Working Days, or such other period agreed with the Buyer, following the Breach of Security, provide to the Buyer:

14.3.1 full details of the Breach of Security; and

14.3.2 if required by the Buyer:

14.3.2.1 a root cause analysis; and

14.3.2.2 a draft plan addressing the root cause of the Breach of Security,

(the "**Breach Action Plan**").

14.4 The draft Breach Action Plan must, in respect of each issue identified in the root cause analysis:

14.4.1 how the issue will be remedied;

14.4.2 the date by which the issue will be remedied; and

14.4.3 the tests that the Supplier proposes to perform to confirm that the issue has been remedied or the finding addressed.

14.5 The Supplier shall promptly provide the Buyer with such technical and other information relating to the draft Breach Action Plan as the Buyer requests.

14.6 The Buyer may:

14.6.1 reject the draft Breach Action Plan where it considers that the draft Breach Action Plan is inadequate, providing its reasons for doing so, in which case:

14.6.1.1 the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Breach Action Plan submit a revised draft Breach Action Plan that takes into account the Buyer's reasons; and

14.6.1.2 paragraph 14.5 and 14.6 shall apply to the revised draft Breach Action Plan;

14.6.2 accept the draft Breach Action Plan, in which case the Supplier must immediately start work on implementing the Breach Action Plan.

Assistance to Buyer

14.7 Where the Breach of Security concerns or is connected with the Buyer Data or the Code, the Supplier must provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction.

14.8 The obligation to provide assistance under paragraph 14.8 continues notwithstanding the expiry or termination of this Contract.

Reporting of Breach of Security to regulator

14.9 Where the Law requires the Supplier report a Breach of Security to the appropriate regulator, the Supplier must:

14.9.1 make that report within the time limits:

14.9.1.1 specified by the relevant regulator; or

14.9.1.2 otherwise required by Law;

14.9.2 to the extent that the relevant regulator or the Law permits, provide the Buyer with a full, unredacted and unedited copy of that report at the same time it is sent to the relevant regulator.

14.10 Where the Law requires the Buyer to report a Breach of Security to the appropriate regulator, the Supplier must:

14.10.1 provide such information and other input as the Buyer requires within the timescales specified by the Buyer;

14.10.2 ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Buyer.

14.11 This Paragraph 14 applies in addition to, and not in substitution of, the Parties' obligations in respect of a Personal Data Breach set out in this Contract..

15. Return and Deletion of Buyer Data

15.1 The Supplier must create and maintain a register of

15.1.1 all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer; and

15.1.2 those parts of the Supplier Information Management System, including those parts of the Supplier Information Management System that are operated or controlled by any Sub-contractor, on which the Buyer Data is stored (the "**Buyer Data Register**").

15.2 The Supplier must:

15.2.1 review and update the Buyer Data Register:

15.2.1.1 within 10 Working Days of the Supplier or any Sub-contractor changes those parts of the Supplier Information Management System on which the Buyer Data is stored;

15.2.1.2 within 10 Working Days of a significant change in the volume, nature or overall sensitivity of the Buyer Data stored on the Supplier Information Management System;

15.2.1.3 at least once every 12 (twelve) months; and

15.2.2 provide the Buyer with a copy of the Buyer Data Register:

15.2.2.1 whenever it updates the Buyer Data Register; and

15.2.2.2 otherwise when the Buyer requests.

15.3 The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code:

15.3.1 when requested to do so by the Buyer; and

15.3.2 using a deletion method agreed with the Buyer that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

15.4 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code:

15.4.1 when requested to do so by the Buyer; and

15.4.2 using the method specified by the Buyer.

Appendix 2 Security Requirements for Development

1. Secure Software Development by Design

1.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, implement secure development and deployment practices to ensure that:

1.1.1 no malicious code is introduced into the Developed System or the Supplier Information Management System.

1.1.2 the Developed System can continue to function in accordance with the Specification:

1.1.2.1 in unforeseen circumstances; and

1.1.2.2 notwithstanding any attack on the Developed System using common cyber-attack techniques, including attacks using those vulnerabilities identified at any time in the OWASP Top Ten.

1.2 To those ends, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:

1.2.1 comply with the Secure Development Guidance as if its requirements were terms of this Contract; and

1.2.2 document the steps taken to comply with that guidance as part of the Security Management Plan.

1.3 In particular, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:

1.3.1 ensure that all Supplier Personnel engaged in Development Activity are:

1.3.1.1 trained and experienced in secure by design code development;

1.3.1.2 provided with regular training in secure software development and deployment;

1.3.2 ensure that all Code:

1.3.2.1 is subject to a clear, well-organised, logical and documented architecture;

1.3.2.2 follows OWASP Secure Coding Practice

1.3.2.3 follows recognised secure coding standard, where one is available;

1.3.2.4 employs consistent naming conventions;

1.3.2.5 is coded in a consistent manner and style;

1.3.2.6 is clearly and adequately documented to set out the function of each section of code;

1.3.2.7 is subject to appropriate levels of review through automated and non-automated methods both as part of:

(a) any original coding; and

(b) at any time the Code is changed;

1.3.3 ensure that all Development Environments:

1.3.3.1 protect access credentials and secret keys;

1.3.3.2 is logically separate from all other environments, including production systems, operated by the Supplier or Sub-contractor;

1.3.3.3 requires multi-factor authentication to access;

1.3.3.4 have onward technical controls to protect the Developed System or the Supplier Information Management System in the event a Development Environment is compromised;

1.3.3.5 use network architecture controls to constrain access from the Development Environment to the Developed System or the Supplier Information Management System;

2. Secure Architecture

2.1 The Supplier shall design and build the Developed System in a manner consistent with:

15.4.3 the NCSC's guidance on "Security Design Principles for Digital Services";

15.4.4 where the Developed System will Process bulk data, the NCSC's guidance on "Bulk Data Principles"; and

15.4.5 the NCSC's guidance on "Cloud Security Principles".

2.2 Where any of the documents referred to in paragraph 2.1 provides for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.

3. Code Repository and Deployment Pipeline

3.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity:

(a) when using a cloud-based code depository for the deployment pipeline, use only a cloud-based code depository that has been assessed against the NCSC Cloud Security Principles;

(b) ensure user access to cope repositories is authenticated using credentials, with passwords or private keys;

(c) ensure secret credentials are separated from source code.

(d) run automatic security testing as part of any deployment of the Developed System.

4. Development and Testing Data

4.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, use only anonymised, dummy or synthetic data when using data within the Development Environment for the purposes of development and testing,

5. Code Reviews

5.1 The Supplier must:

5.1.1 regularly; or

5.1.2 as required by the Buyer

review the Code in accordance with the requirements of this paragraph 5 (a "**Code Review**").

5.2 Before conducting any Code Review, the Supplier must agree with the Buyer:

5.2.1 the modules or elements of the Code subject to the Code Review;

5.2.2 the development state at which the Code Review will take place;

5.2.3 any specific security vulnerabilities the Code Review will assess; and

5.2.4 the frequency of any Code Reviews (the "**Code Review Plan**").

5.3 For the avoidance of doubt the Code Review Plan may specify different modules or elements of the Code are reviewed at a different development state, for different security vulnerabilities and at different frequencies.

5.4 The Supplier:

5.4.1 must undertake Code Reviews in accordance with the Code Review Plan; and

5.4.2 may undertake Code Reviews by automated means if this is consistent with the approach specified in the Code review Plan.

5.5 No later than 10 Working Days or each Code Review, the Supplier must provide the Buyer will a full, unedited and unredacted copy of the Code Review Report.

5.6 Where the Code Review identifies any security vulnerabilities, the Supplier must:

5.6.1 remedy these at its own cost and expense;

5.6.2 ensure, so far as reasonably practicable, that the identified security vulnerabilities are not present in any other modules or code elements; and

5.6.3 modify its approach to undertaking the Development Activities to ensure, so far as is practicable, the identified security vulnerabilities will not re-occur; and

5.6.4 provide the Buyer with such information as it requests about the steps the Supplier takes under this paragraph 5.6.

6. Third-party Software

6.1 The Supplier must not, and must ensure that Sub-contractors do not, use any software to Process Buyer Data where the licence terms of that software purport to grant the licensor rights to Process the Buyer Data greater than those rights strictly necessary for the use of the software.

7. Third-party Software Modules

7.1 Where the Supplier or a Sub-contractor incorporates a Third-party Software Module into the Code, the Supplier must:

7.1.1 verify the source and integrity of the Third-party Software Module by cryptographic signing or such other measure that provides the same level of assurance;

7.1.2 perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Software Module;

7.1.3 continue to monitor any such Third-party Software Module so as to ensure it promptly becomes aware of any newly-discovered security vulnerabilities;

7.1.4 take appropriate steps to minimise the effect of any such security vulnerability on the Developed System.

7.2 The Supplier must produce and maintain a register of all Third-party Software Modules that form part of the Code (the "**Modules Register**").

7.3 The Modules Register must include, in respect of each Third-party Software Module:

7.3.1 full details of the developer of the module;

7.3.2 the due diligence the Supplier undertook on the Third-party Software Module before deciding to use it;

7.3.3 any recognised security vulnerabilities in the Third-party Software Module; and

7.3.4 how the Supplier will minimise the effect of any such security vulnerability on the Developed System.

7.4 The Supplier must:

7.4.1 review and update the Modules Register:

7.4.1.1 within 10 Working Days of becoming aware of a security vulnerability in any Third-party Software Module; and

7.4.1.2 at least once every 6 (six) months;

7.4.2 provide the Buyer with a copy of the Modules Register:

7.4.2.1 whenever it updates the Modules Register; and

7.4.2.2 otherwise when the Buyer requests.

Appendix 3 Security Working Group

1 Role of the Security Working Group

1.1 The Security Working Group shall be responsible for the administration and governance of security, data protection and cyber security matters throughout the lifeline of the contract period.

1.2 The Security Working Group:

(a) monitors and provides recommendations to the Supplier on the Buyer-led Assurance of the Supplier Information Management System; and

(b) will operate in accordance with the terms of reference notified by the Buyer to the Supplier from time to time (with the version at the Start Date titled “GDS Information Assurance: DI Security Working Group Terms of Reference” dated July 23 as provided to the Supplier prior to the Start Date). .

2 Meetings of the Security Working Group

2.1 Paragraph 4 of Call Off Special Schedule 8 (Call Off Contract Management) shall apply to the Security Working Group as if it were a Board established under that Schedule.

3 Reports to the Security Working Group

3.1 The Supplier must provide the following reports no late than five Working Days before each meeting of the Security Working Group:

(a) The initial SWG will review the content of the Security Management Plan for subsequent actions to be agreed.
(b) Regular SWG’s will be supported by agreed Agenda and Actions for update.

4 Administration

4.1 The Buyer is responsible for the secretarial functions of the SWG.

Appendix 4 Sub-contractor Security Requirements and Security Requirements for Development

The table below sets out the Security Requirements and Development Requirements that do **not** apply to particular categories of Sub-contractors.

	SIMS Sub-contractors	**Higher Risk Sub-contractors**	**Medium Risk Sub-contractors**	**Sub-contractors**
Security Requirements that do not apply				
Development Requirements that do not apply				

Appendix 5 Security Management Plan Template

Issued to the Supplier separately.

Call Off Special Schedule 2 – Buyer Requirements

1. General requirements

1.1. General Requirements

The below requirements provide a high-level overview of the requirements that shall apply with effect from the Service Commencement Date.

ID	Requirements Description
1CCP001	The Supplier shall provide a single Contact Centre service, with related administrative and processing services, for all Users of GOV.UK One Login Platform as outlined in 'RM6181 Framework schedule 1 (specification)'.
1CCP002	The Supplier shall provide all necessary facilities, systems, infrastructure and security cleared staff necessary to provide a Contact Centre service throughout the life of the contract. (National Security Standards) The parties acknowledge that certain staff members of the Supplier may require Security Clearance (SC) prior to the commencement of Phase 2 work. In such cases, the Buyer and Supplier shall enter into a separate agreement to facilitate the necessary SC clearance process. The terms and conditions of this separate agreement shall be mutually agreed upon by the Buyer and Supplier, outlining the responsibilities, timelines, costs, and any other relevant considerations related to the SC clearance process
1CCP003	The Supplier should have, from the launch of the Contact Centre, a WebChat capability to support Users using the link on GOV.UK.
1CCP004	The Supplier will be required to provide contact handling across voice, webchat, email, messaging and other web-based channels including chatbot and social media platforms, including (but not limited to) Facebook, WhatsApp, Twitter, etc.
1CCP005	The Supplier shall provide and use 0300 numbers for Users based in the UK and an international version of the contact no. for the Users based outside of the UK.

1CCP006	The Supplier must comply with the requirements of the Welsh Language Act 1993 by providing a Welsh speaking IVR, chatbot, webchat and email channels and contact centre agent to Users requiring this service.

1.2. Target User Base

The below requirements refer to the inclusivity of all Users that the Supplier needs to facilitate through the Contact Centre.

<table>
<tr><th>ID</th><th>Requirement Description</th></tr>
<tr><td>2CCP001</td><td>The Supplier will support the Government Digital Inclusion Strategy to promote digital inclusion and therefore provide a service that will meet all User segment's needs as outlined below
<table>
<tr><th>User Segment</th><th>Definition</th></tr>
<tr><td>Non-digital User</td><td>The segment of Users who are not technical or knowledgeably equipped to use Information and Communications Technologies ('ICT'). Includes also the section of the population which has access to the ICT, but which is not willing to use them or lacks the resources to access digital content.</td></tr>
<tr><td>Low Digital Skilled User</td><td>The section of the population which has access to the ICT, and wants to use them but has limited digital skills.</td></tr>
<tr><td>Digital User</td><td>The section of the population able to use digital devices (such as computers or smartphones and the internet.), to gain access to essential services.</td></tr>
</table></td></tr>
</table>

2CCP002	The Supplier will facilitate the evolution of security capabilities to provide a fuller service offering for the User Segments as the scope of the Contact Centre changes in phases 2 and 3. For instance potentially implement security screening, if needed to support Non-digital Users following sufficient demand cost-benefit analysis see (see requirement 17CCP001 for future phases' outcomes.
2CCP003	The Supplier shall provide assistive technologies to support Users who may have impairments or disabilities so that these Users are serviced successfully, experience positive engaging interactions and are digitally included in line with 'RM6181 Framework schedule 1 (specification).'
2CCP004	The Supplier must provide a capability to identify whether a User is vulnerable across channels so that the vulnerable Users can be assisted appropriately.
2CCP005	The Supplier will offer support and communication across all diversity target and vulnerable groups
2CCP006	The Supplier will comply with the "The Public Sector Bodies (websites and Mobile Applications) (No 2) Accessibility Regulations. The Supplier to demonstrate WCAG 2.1 standards and to confirm status in contract requirements.

1.3. How the Contact Centre fits in with the Buyer Operating Model

ID	Requirement Description
3CCP001	The Supplier will provide a Contact Centre that will be the first point of contact for all Users that need support for sign ups / sign ins related queries.
3CCP002	The Supplier will escalate technical issues when needed by exception to the Technical Service Desk.
3CCP003	The Supplier should ensure that the Contact Centre solution is interoperable across other Buyer solutions) and supports the triage and escalation of tech issues to the Technical Service Desk, including integrating the Contact Centre's Service CRM platform with the Buyer's ITSM tool (using standard APIs for integration), and handoff

	options (as outlined in requirement 6CCP002) to support RPs to provide a consistent and seamless user experience.
3CCP005	The Supplier shall manage various hand off options to RPs in accordance with the agreed hand off requirements for the RPs depending on their service strategy.
3CCP006	The Supplier will need to hand off in the agreed variation from Service A, B and C at MVP (Phase 1). Then later on, evolve to support the hand off Service D and E in the below (as outlined in requirement 6CCP002) when appropriate based on demand and cost-benefit analysis.
3CCP006	The Supplier will work with the Buyer and RPs as required to determine which hand-offs variations, as outlined in requirement 6CCP002, are best practice for handing off to the RPs in terms of cost and balancing failure demand.
3CCP007	The Supplier will provide a triage process plan for all relevant technical issues that need to be escalated to the Technical Service Desk via using an agreed technologies and platform.

2. Detailed requirements

2.1. User Support Service Experience, Contact Management and Complaints

2.1.1. User Support Service Experience

These requirements reference the user support experience that the contact centre will be providing to Contact Centre Users.

ID	Requirement Description
4CCP001	The Supplier shall provide a solution that delivers an Omni-Channel experience for Users.
4CCP002	The Supplier will provide a service which supports the Buyer' mission statement to provide 'a simple, joined-up and personalised experience of government services to everyone'.

4CCP003	The Supplier shall provide a consistent experience across the following channels: Inbound: Telephony, Webchat, Email, Social Media. Outbound: SMS, Email, Social Media.
4CCP004	The Supplier shall adopt a "right first time" approach to ensure that avoidable repeat User contact is reduced; this will be measured against the Service Level 18 in 'Call off Schedule 14 - Service Levels'.
4CCP005	The Supplier shall work in collaboration with the Buyer in encouraging Users to use the digital identity verification channels, as opposed to in-person verification in first instance and when appropriate.

2.1.2. Contact Management

The Contact Centre is expected at launch to deal with most queries and be able to redirect to specific departments when needed appropriately. It is expected that User contacts are handled professionally, courteously and promptly in line with 'Call off Schedule 14 - Service Levels.'

These requirements cover the particular inquiries that contact centre agents will be required to answer.

ID	Requirement Description
5CCP001	The Supplier will ensure the Contact Centre is the first point of contact for support at launch MVP, Phase 1 for the following GOV.UK One Login use cases: 1. Account Creation: Sign up, Sign in, Authentication (Email and mobile no.), MFA Method, Tech Issues, Account Sign in, Password reset, Forgot email address, Tech issues. 2. Prove Your Identity: Scanning Doc. and NFC, Required documents, online verification, Reuse of identity verification, Online Verification process, Timeline for the outcome, Tech issues. 3. Account management: Update account details, Change email address, Change password, Delete account, Change MFA Method

	4. View My Activity: Access to account history, Report fraud/ suspicious activity, Tech Issues 5. Face-to-Face Journey, Guidance around F2F Process, Tech issues. 6. Policy Hand Offs: Queries related to RPs policy.
5CCP002	The Supplier will provide a Contact Centre which will have the following in scope for launch MVP, Phase 1: ● Direct the User to Self-Serve. ● Guide the User through the verification process. ● Hand off to other RPs (e.g. HMRC, DVLA etc.) recognising the different expectations for Digital and Non-digital Users (hand off examples are set out at requirement 6CCP002 below). ● Triage tech and fraud queries. ● Inform the User of the different verification methods they can pursue (e.g. App, F2F etc.) ●
5CCP003	The Supplier must be able to change the content of all User contact messaging formats (e.g. text, webchat, chatbot and email templates) and inbound call routing process, when advised to do so by the Buyer. There shall be urgent and standard timeframes based on ITIL Change Management Process.
5CCP004	The Supplier shall set up (Role Based Access Control) RBAC and channels for the staff.
5CCP005	The Supplier will provide the ability to accept Users queries via multiple channels and send outbound emails to Users when appropriate.

2.1.3. Complaints

These requirements cover the minimal process required to be in place for when the Contact Centre deals with complaints and escalations about its service (a complaint is an expression of dissatisfaction could be oral / written).

It is expected that user contact complaints are handled professionally, courteously, promptly, with empathy and shall be escalated when appropriate.

During the planning phase of the project, both parties acknowledge and agree that specific complaint methods and procedures for addressing customer queries and concerns shall be determined and documented in a mutually agreed-upon plan. While the precise details of the complaint methods are not currently known, the parties commit to working together to establish clear and effective processes for handling customer complaints. Both parties shall actively participate in the planning phase to identify, define, and agree upon the complaint methods, including the channels of communication, escalation procedures, response times, and any other relevant considerations.

ID	Requirement Description
6CCP001	The Supplier shall record and resolve complaints about the contact centre service in line with 'Call off Schedule 14 - Service Levels' and within an agreed complaints framework to ensure a seamless user support experience.
6CCP002	The Supplier will handle all User complaints related to the Identity Verification process and will redirect any complaints that relate to a Government Service (RPs) in the agreed hand off variation. The hand off variations are outlined as per the below, but not limited to: - Agent transfers user to an RP live agent - Agent transfers user to the RPs support channel - Agent shares relevant RP service contact information - Agents tells user to go to the relevant RPs gov.uk website - Agents tells user to go elsewhere
6CCP003	The Supplier shall design and deliver a defined complaints escalation process which is clear for agents to follow so they can effectively escalate complaints to the appropriate channels.
6CCP004	The Supplier will deliver a complaint management process service that supports effective ownership of reported issues.

6CCP005	The Supplier shall design and employ appropriate methods to manage policy/large incident related complaints so they can be dealt with.
6CCP006	The Supplier will have an effective and proactive root cause management and analysis capability for complaints, so that trends can be easily identified and addressed to continuously improve service.
6CCP007	The Supplier will escalate Phishing attempt complaints to the Technical Service Desk when appropriate.
6CCP008	The Supplier will train its user support staff on the organisation's complaints procedure in line with their own organisation's written policies and, at a minimum, the following training should be covered: ● Complaint identification ● Complaints recording – accuracy of this recording ● Complaints resolution / handling difficult Users ● Complaints procedure ● Escalation process
6CCP009	The Supplier shall provide data, reporting and insights to ensure complaint volumes and reasons are understood by the Buyer's senior leadership.

2.2. Resourcing and Training

These requirements refer to the required employee experience and training that the contact centre will provide.

ID	Requirement Description
7CCP001	The Supplier shall provide their hybrid working plan and ensure the tech and working environment is secure in line with security requirements.

7CCP002	The Supplier will provide a multiskilled user support team who are able to answer inbound calls, chats and emails, social media and have suitable knowledge of the Buyer and the systems.
7CCP003	The Supplier will be responsible for recruiting and onboarding suitable staff to provide high quality user support experience with the appropriate JML (Joiners, Movers, Leavers) processes in place in line with 'RM6181 Framework schedule 1 (specification)'
7CCP004	The Supplier shall provide a training plan and be responsible for training contact centre agents using training content to be agreed with the Buyer, as referenced in MD14 within 'Call-Off Schedule 3 Continuous Improvement 2.3.'
7CCP005	The Supplier should develop the Knowledge Based Articles and use that to train the agents working with the Buyer teams to understand the product to help build the articles, with the Buyer teams providing relevant product documentation.
7CCP006	The Supplier will be responsible for providing training on the below (outlined within the Training Plan deliverable), in accordance with the Buyer's reasonable instructions, to new staff and ongoing training needs including but not limited to: ● New processes ● Updates ● Systems ● Fraud ● Data Management ● User Service ● Inclusivity and Sensitivity ● Information Security
7CCP007	The Supplier will provide a resource allocation plan detailing how the team may be assigned to different skills/channels e.g. voice vs non-voice.

7CCP008	The Supplier will manage staff engaged in the delivery of the Services in accordance with Good Industry Practice . In particular (but without limitation) the Supplier shall use all reasonable endeavours to achieve: ● staff turnover rates; and ● a mix of staff who are permanently employed and staff engaged on temporary contracts that are comparable with and do not substantially exceed the rates and proportions that are consistent with Good Industry Practice.

2.3. Technical (system) Requirements

These requirements relate to the Technical System Requirements for the contact centre solution, these are in addition to the minimum outlined under section 4.4. Technology in 'RM6181 Framework schedule 1 (specification)'.

ID	Requirement Description
8CCP001	The Supplier shall design and perform testing to demonstrate the efficacy, functionality, usability and completeness of the programme requirements before implementation and prior to go live with Buyer acceptance of service process defined.
8CCP002	The Supplier must ensure Service interactions within the solution Platform will be traceable and can be monitored end to end.
8CCP003	The Supplier shall deliver a Contact Centre technology solution to support the Buyer's GOV.UK One Login programme in accordance with these requirements.
8CCP004	The Supplier shall provide the tools and technologies to effortlessly route and handle all Inbound/Outbound User interactions. ● Automatic Call Distribution (ACD)

	• Work Item • Dialer
8CCP005	The Supplier should provide the intelligent solutions that improve every experience by supporting below technologies. • Intelligent Instant Voice Response • Virtual Agent • Agent Assist
8CCP006	The Supplier must provide an contact centre solution which supports the wider technology ecosystem: • Dynamic Integration Framework • Open API • Software Development Kit (SDK) • Team Messaging • Manage and provide Reachback solutions for legacy systems • Ability to onboard and manage legacy systems • Data Management Services (Database Management, Capacity Management, Data Migration Support, Data Warehouse Management, Architecture Support). • Customer Relationship Management and Enterprise Resource Management. • Change management process. • NCSC Cloud Security Principles • Cyber Security Protections • All agent hardware devices for Phase 1
8CCP007	The Supplier will deliver an interoperable contact centre solution across other Buyer solutions, that supports the triage and escalation of tech issues to Technical Service Desk and handoff options (as

	outlined in requirement 6CCP002) to support RPs to provide a consistent and seamless user experience.
8CCP008	The Supplier will provide a technical solution and platform with below reporting and analytics capabilities to promote the transparency of volume metrics and insights to executive stakeholders. ● Contact Centre Service Level Reporting ● Real-time Dashboards ● Interaction Journey Analytics ● Surveys ● Speech and Text Analytics ● Sentiment analysis for improved User service ● Access to raw data if needed
8CCP009	The Supplier shall provide a contact centre solution which has capabilities to integrate with below systems, but not limited to. ● Current AWS services, including using AWS IAM ● AWS cloudwatch and Dynatrace using kinesis ● Zendesk and future service desk platforms ● Lex

2.4. Security and fraud management

The Buyer requires that its contact centre services are secure, maintain data integrity and support data protection see also ‘Special Schedule 1 (Security Management)’.

They must be provided via an assured solution.

ID	Requirement Description
9CCP001	The Supplier shall actively detect, monitor for fraudulent activity and report suspicious trends including but not limited to the below:

	● inbound identity misuse, ● service denial, ● account hijacking, ● phishing, ● other fraudulent types of activity For priority cases the Supplier will report via escalation routes to the Service Desk, the Buyer's Fraud and Security Team.
9CCP002	The Supplier shall operate their own fraud monitoring systems and security monitoring systems with processes and escalation routes that will be agreed with the Buyer and in line with recognised standards and industry best practices. The Supplier shall share details of any attempted fraud or suspicious activities detected in its systems and processes or in relation to the Services, where lawful and proportionate to do so.
9CCP003	The Supplier shall share all fraud signals (flags to accounts) with the Buyer fraud analysts via a secure method that is agreed with the Buyer and in line with recognised standards and industry best practices.
9CCP004	The Supplier's scripts and processes will be reviewed from a fraud perspective, with the Buyer able to have sight and review them too.
9CCP005	The Supplier shall confirm the User being interacted with is the owner of the account, before changing any account details using the security screening platform if determined necessary for future evolutions of the contact centre.
9CCP006	The Supplier shall provide logs and event data to the security monitoring solution within an agreed Service Level (as per Service Level 26), so that attacks can be detected and responded to in a timely manner. The Supplier will present details on how this data will flow into the security monitoring system.

9CCP007	The Supplier will train agents on detecting fraudulent activity in-line with the Buyer's expectations (as per Service Level 28).
9CCP008	The Supplier shall ensure that any staff associated with the Buyer's Contact Centre contract are cleared to the following Security Levels, as appropriate: • All User Support Agents from MVP Phase 1 must be cleared to Baseline Personnel Security Standard (BPSS) level and do not need to be seated in a segregated area.
9CCP009	The Supplier shall ensure that any identified staff for roles associated with the Buyer's Contact Centre in Phases 2, 3 + be cleared to higher Security levels as per UK National Security Guideline (CTC or SC) as requested by the Buyer and will have Buyer managed devices as requested by the Buyer. The Supplier and the Buyer shall also agree to segregated seating for these same roles / agent groups.
9CCP010	The Supplier will respond to any lawful request from UK Law Enforcement or the UK Intelligence service(s) for the acquisition of communications data for detection, prevention or prosecution of crime. In accordance with but not limited to the Investigatory Powers Act (IPA) 2016 and the Regulation of Investigatory Powers Act 2000 (RIPA) and in the event the request has not come from the Buyer, they will notify the Buyer provided there are no lawful reasons prohibiting this
9CCP011	The Supplier will do the following in accordance with the relevant Service Levels 'Call off-Schedule 14 - Service Levels' decided in implementation: • Check User data for fraud indicators • Flag possible fraud cases on a continual basis • Tackle sleeper or breakout fraud
9CCP012	The Supplier will ensure they have the appropriate mechanisms in place for sharing data in a secure manner and receiving and handling requests related to suspicious activity from a User and from the Buyer

9CCP013	The Supplier shall manage all fraud related activities including, contact centre fraud (implement training) and implement Anti- Fraud Detection processes and technologies to mitigate both User fraud and internal fraud.
9CCP014	The Supplier must have the ability to provide and / or integrate additional counter fraud response technologies e.g. Nuance Bad Voice, Pindrop etc.
9CCP015	The Supplier will deploy the latest versions (n-1) of all of the commodity components, such as operating systems, web development frameworks and latest version of security patches, to ensure you benefit from the latest security features.
9CCP016	The Supplier must conduct regular professional penetration testing, at least once a year on the anniversary of the Service Commencement Date, to verify that the services being provided are secure before going live and on an ongoing basis as reflected within the Call off Security Schedule 9
9CCP017	The Supplier shall provide contact centre services, including any interfaces to the Buyer and third-party Supplier systems (as referenced throughout this document), via a resilient and security assured solution approved by the Buyer. Security standards are set out in 'Special Schedule 1 (Security Management)'.

2.5. Quality Standards

The Buyer expects a Contact Centre that supports its mission to deliver ‘a simple, joined-up and personalised experience of government services to everyone’. These requirements incorporate how the Supplier should be able to demonstrate that this has been achieved.

ID	Requirement Description
10CCP001	The Supplier shall be responsible for conducting internal call, conversation and email monitoring to ensure quality of service is maintained in line with the agreed baselined standards and ‘Call off Schedule 14 - Service Levels’, across all contact channels.
10CCP002	The Supplier and the Buyer will work together to review ‘Call off Schedule 14 - Service Levels’, every 6 months to determine if they are still appropriate and suitable and if not will mutually agree revised SLAs fit for purpose.
10CCP003	The Supplier will provide regular reports on both agent and departmental performance and development areas.
10CCP004	The Supplier shall follow ITIL Best Practice guidelines for the provision and support of all services.
10CCP005	The Supplier shall deliver Contact Centre services in compliance with relevant quality standards as documented at ‘Call off Schedule 14 - Service Levels’.
10CCP006	The Supplier shall comply with the Plain English Campaign (www.plainenglish.co.uk) and Welsh Standards Language guidelines.
10CCP007	The Supplier shall provide details of any certification/assurance held regarding industry quality standards and detailed plan to outline how these will be maintained throughout the period of the contract.

2.6. Continuous Improvement, Innovation, Savings and Efficiency.

These requirements refer to the need for continuous improvement and management of innovation to be embedded into the delivery of the services. It is expected that this will result in savings, efficiencies and quality improvements.

It is also expected that the Supplier will work in collaboration (as outlined below in 3.4.1) and support the Buyer in its commitment to provide better digital services to Users.

ID	Requirement Description
11CCP001	The Supplier, in line with 'Call off Schedule 3 - Continuous Improvement', shall embed Continuous Improvement and Innovation working patterns into the delivery of the services to ensure lower costs, savings and efficiencies, and improvements to quality of service over the life of the contract - including maximising inclusion. This will be evidenced in the form of a Continuous Improvement and Innovation Plan (as referenced in Call-Off Schedule - Continuous Improvement 3 2.3 within the MD05 deliverable).
11CCP002	The Supplier shall follow continuous improvement principles in developing the service requirement. For example, the Supplier must keep up with technological advances in Contact Centre strategies, present any ideas for service innovation with the associated benefits (such as reduced avoidable contact or contact duration) to the Buyer and continuously develop their team to ensure they are in line with industry best practice.
11CCP003	The Supplier will have regular (weekly) contact with the Service Desk, feeding back any issues and common topics raised by Users, with the focus on continual service improvement.
11CCP004	The Supplier will keep a record of common User topics that can be fed back so the focus is on continual improvement at programme level.
11CCP005	The Supplier shall identify and quantify the impact of changes in systems across the Contact Centre platform and work with the Buyer and other RPs to maintain suitable test environments of dependent and/or associated system functionality to enable full end to end testing of changes originating in adjacent systems.
11CCP006	The Supplier will use complaints analysis to provide feedback and recommendations to the specific Buyer departments / staff so that complaint repeats can be avoided, and user experience can be continually improved.

11CCP007	The Supplier will create and maintain a communication plan for regular communication with the Buyer's product teams. This will be used for feedback about complaints (data insights and analysis) for the product content manager to update self-serve content.

2.7. Collaboration with the Buyer - Ways of Working - Test and Learn Approach Which User journeys cases need to be prioritised

The following requirements refer to the collaboration approach that the Supplier will take when working with the Buyer throughout the contract. In line with 'RM6181 Framework schedule 1 (specification'.

ID	Requirement Description
12CCP001	The Supplier will work in collaboration with the Buyer following the below principles: ● Align with the Buyer's strategic goals as listed in 3.2.1 and collaboration principles as detailed below: ○ Collaboration Principles ○ Frequent communication to establish and maintain an open, productive and mutual trust relationship with communications at all levels and transparency throughout. ○ Mutual investment in value creation with shared collaboration initiatives that improve overall performance. This can include, but is not limited to, co-locating key staff at regular intervals, regular site visits, interactive workshops to share insights and drive innovation. ○ Work closely together to identify and address potential and actual problems. Have a joint approach to risks and issues. ○ Align with the Buyer's strategic goals ○ Deliver on organisational governance - , for example, with an Executive Committee, Relationship Management, Operations Support Transformation Office, Delivery,

	Security Management Group etc. be proactive in sharing ideas and progress metrics as outlined in 'Call off Schedule 14 Service Levels' and Annex A. ○ Have knowledge of the key stakeholders, contact points and how to interact with each other. ○ The Buyer's Executives may express interest in performing service tasks at their discretion, acting as service agents. The Contractor will grant these senior executives the necessary authorisation and authority to act as service agents in accordance to the requirements. ● Deliver on value creation and sharing - share collaboration initiatives that improve overall performance. ● Work together to manage potential and actual problems. Have a joint approach to risks and issues. ● Have an open, productive and mutual trust relationship with communications at all levels and transparency throughout. ● Joint focus on working proactively and sharing ideas to achieve the inclusivity business objectives as outlined in 3.2.4.
12CCP002	The Supplier will work in collaboration with the Buyer to develop analysis to determine whether the potential future scope features of the Contact Centre outlined in 16CCP001 are viable and needed.

2.8. Data integrity and Data Protection

The Buyer requires that its Contact Centre services are secure, maintain data integrity and support data protection. They must be provided via an assured solution.

ID	Requirement Description
13CCP001	The Supplier shall follow good security practice and maintain data integrity, as defined in the NCSC CAF and comply with all UK's applicable Data Protection Legislation during implementation and through the life of the contract. This is to enable business operations to be conducted in a secure manner in line with requirements and

	standards as outlined in 'RM6181 Joint schedule 11: processing data v4.2' and 'Special Schedule 1 (Security Management)'.
13CCP002	The Supplier will ensure that User access to the systems and applications is authenticated, authorised and logged so that the confidentiality, integrity and availability can be maintained and audited during the life of the contract.
13CCP003	The Supplier shall ensure that information is exchanged securely with other services within the government, so that the confidentiality, integrity and availability of the solution and its information is protected at all times.
13CCP004	The Supplier will ensure that there is effective data management and it is available to the right people at the right time on Roles Based Access Control (RBAC). RBAC will be defined at a granular level such that privileged Users will not be able to access data that is not required for their role or the cases they are working on. The Supplier must provide a proposed RBAC process for approval by the Buyer.
13CCP006	The Supplier shall record and securely store all inbound and outbound User contacts across all channels for audit, training, quality control and security purposes with access on request by the Buyer within 24 hours.

2.9. Business Continuity/Disaster Recovery

The Buyer require that the Supplier has a business continuity and disaster recovery plan in place to ensure that business continuity is maintained and disaster recovery supported with minimal disruption to the delivery of Contact Centre services.

ID	Requirement Description
14CCP001	The Supplier shall have and maintain a Business Continuity and Disaster Recovery plan (BCDR Plan) as outlined in 'Call off Schedule 8 - Business Continuity and Disaster Recovery' .
14CCP002	The Supplier shall support RPs individual BCDR needs as they onboard, and develop a BCDR plan that is able to meet expectations once these needs are understood. This may include a range of alternative strategies that can handle even the most severe situation,

	ensuring there are no outages in user support in the event of an unexpected crisis.
14CCP003	The Supplier shall provide a detailed risk analysis and a joint risk management process.
14CCP004	The Supplier shall provide notification to the Buyer of all planned and unplanned service outages and service disruptions within a timescale to be agreed with the Buyer as per the BCDR Plan. This will be followed up by an incident report that will include lessons learnt and action to be taken.
14CCP004	The Supplier shall provide resilient solutions so that services to the Users are available as agreed in the 'Call off Schedule 14 - Service Levels'.
14CCP005	The Supplier shall follow the established escalation process to successfully report and navigate any error/issue that is deemed an incident.
14CCP006	The Supplier shall have access to the IT Service Management system and a Knowledge Base in order to check whether incidents are already known and report incidents to the appropriate channels.
14CCP007	The Supplier shall undertake and share outcomes of regular response exercises based on scenarios, annually.

2.10. Infrastructure

The below requirement refers to the location of the Contact Centre.

ID	Requirement Description
15CCP001	The Supplier will provide and manage a Contact Centre service, working closely with the Buyer's Operations hub located in Manchester in keeping with the principles laid out on Section 3.4.1, "Collaboration with the Supplier." The Supplier should indicate where it would base the One Login Contact Centre and set out a proposal for how they will enable an effective partnership, including regular colocation between the Buyer's staff and Supplier's staff, facilitate hosting of key meetings, and allow

	the Buyer to conduct regular site inspections and monitoring sessions. The Supplier should expect a higher frequency of such interactions during initial implementation and immediately before and after the onboarding of new services or introduction of new functionality, with a reduction in frequency once operational performance has been demonstrated. The expected meeting cadence and attendance for such visits will be detailed in Call Off Schedules 13 and 20.
15CCP002	The Supplier needs to ensure that all processing of data whether hosting, secure servers, data centres or security of processing must be undertaken within the UK only under GDPR policies (Which specifies that the definition of Data Processing Art 4 (2) is ;(2)'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction).

2.11. Support Services

This requirement is in reference to the support services that the Supplier will need to provide to support their Contact Centre Solution.

ID	Requirement Description
16CCP001	The Supplier will provide support services which include but are not limited to the below as outlined in 'RM6181 Framework schedule 1 (specification)' : ● Payroll ● HR ● ICT ● Helpdesk support for Agents.

2.12. Potential Future Developments

2.12.1. Future Scope of the Contact Centre

The below requirements outline the potential future scope of the Contact Centre in phases 2 and 3. Such requirements shall be subject to discussion between the parties under the Variation Procedure (including to identify when the Supplier can start charging for phase 2 and 3 development work).

ID	Requirement Description
17CCP001	The Supplier shall work in collaboration with the Buyer to validate the need for the future requirements in the phases. The validation exercise will comprise of business insights analysis and cost/benefit analysis. Based on the outcome of this the Supplier will determine an implementation plan that can achieve the following outcomes: 1. The agent can validate the identity of the User they are interacting with e.g KBV security screening. 2. Delete accounts on behalf of the User 3. Reset passwords securely 4. Co-browse / screen share with the User 5. Refer the User to the nearest Post Office for F2F verification. 6. Update email address / phone number / contact details on behalf of the Users 7. Update MFA options on behalf of the User. 8. Assist User with account recovery 9. Create account for an assisted digital route for Users with low DI scores or without a mobile phone 10. Completing the process of ID verification on behalf of the User. 11. Agents can respond to User requested call-backs with outbound calls

	12. Agents can respond to emails sent by Users 13. Agents can complete F2F forms on behalf of the User. 14. Screen share and control of the User's screen. 15. Agents can support Users through the vouching process 16. Agents can support Users through the F2F process. 17. Provide additional language support 18. Real-time multilingual chatbot 19. Any other suggestions both from the Supplier and the Buyer.
17CCP002	The Supplier will use the cost/benefit analysis as a roadmap of what requirements are needed and the prioritisation of this will be decided by the Buyer.
17CCP003	The Supplier shall confirm the User being interacted with is the owner of the account, before changing any account details using the security screening platform if determined necessary for future evolutions of the Contact Centre.
17CCP004	The Supplier will propose their approach, with an Implementation and Transition Plan detailing how they would work with the Buyer to transition from Phase 1 and scale to support additional functionality as set out in Phase 2 and 3, including a timeline and milestones from the transition.

The Supplier will demonstrate how they will approach the development of the future feature sets, including providing implementation plans that outline technical and operational development (including resource plans) supported with a pricing schedule that provides a breakdown of all costs of components.

2.12.2. Governance and Transformation Management

These set of requirements refer to the proposed governance and transformation management needed for the Contact Centre solution as it evolves to phases 2 and 3

ID	Requirement Description
18CCP001	The Supplier shall work in collaboration with the Buyer to understand together how extra functionality of the Contact Centre is agreed and built to include necessary programme and transformation requirements into the road map in accordance with a proposed governance model which will be agreed by both parties.
18CCP002	The Supplier shall share the governance plan for review and approval for the Buyer to understand how they will help in supporting the transformation of the Contact Centre and how they will support the governance model outlining oversight layer for the programme

2.13. Non-functional Requirements

These requirements refer to the operating hours of the Contact Centre function, the requirement to be flexible and be scalable in order to meet evolving business needs and deal with the peaks and troughs of demand.

ID	Requirement Description
19CCP001	The Supplier shall operate a full contact centre service during the following opening hours: • Monday to Friday from 08:00 to 20:00 • Saturday, Sunday and standard UK Bank Holidays from 09:00 to 17:30 • 365 days per year (366 days per year for a leap year) • Hybrid Working • 24/7 Support Model (auto-replies, chatbot) • This will be the same for all contact channels.
19CCP002	Opening hours must be reviewed periodically in line with User contact trends analysis and missed opportunity reports.

19CCP003	The Supplier shall be flexible to support the requirement for in-person 24/7 support if needed in future based on demand. This will be managed through the Change Control process.
19CCP004	The Suppliers solution must be flexible to respond and charge accordingly to evolving User demand and changing business needs across all channels, as service volumes may fluctuate due to seasonality.
19CCP005	The Supplier shall provide a scalable operation and technology infrastructure that will be able to manage changes in User demand (within a 30% variance) and will support evolving services across all contact channel types i.e. tactical flexibility to provide immediate operational capability in line with 'RM6181 Framework schedule 1 (specification)'
19CCP006	The Supplier shall provide all infrastructure and development environments required (hardware and software) so that the platform is not reliant on the provided infrastructure.
19CCP007	The Supplier shall provide the capability to record, prioritise and assign issues received via all channels received, ensuring they are resolved promptly and in accordance with the priority set.
19CCP008	The Supplier shall enable the Buyer or a designated third party selected by the Buyer , to undertake call monitoring of live User contacts and recorded User contacts.
19CCP009	The Supplier will be responsible for continually developing the chatbot's capabilities and knowledge to increase the amount of queries it can support and increase its containment rate.

2.14. Social Value

The Buyer requires its Contact Centre Service to follow the PPN/20 guidance for social values as updated along with contributing to the Government's Sustainability Agenda as outlined in the Government's Environmental Policy and Sustainable Development Plan, Outsourcing Playbook, Sustainable Government Buying Standards and 'RM6181 Framework schedule 1 (specification)'

ID	Requirement Description
Sustainability	
20CCP001	The Supplier shall, where possible, provide and deliver products which are environmentally friendly, reusable and recyclable at end of use.
20CCP002	The Supplier shall, as part of continuous improvement and innovation, drive down the use of non-environmentally friendly options and inform the Buyer accordingly.
20CCP003	The Supplier shall complete the Corporate Assessment of Environmental, Social, and Economic Responsibility (CAESER) assessment.
Climate Change	
20CCP004	The Supplier shall encourage environmental protection and improvement, through driving down non-environmental options and providing and delivering products which are environmentally friendly, reusable and recyclable at end of use including working towards net zero greenhouse gas emissions.
20CCP005	The Supplier shall influence staff, sub-Suppliers, Users and communities through the delivery of the contract to support environmental protection and improvement.
Tackling economic inequality	
20CCP006	The Supplier shall support the local communities, through creating opportunities, offering employment and training opportunities in high growth sectors.
Equal opportunity	
20CCP007	The Supplier shall help in reducing the disability employment gap through increasing the representation of disabled people in the contract workforce and supporting them in developing new skills relevant to the contract, including through training schemes that result in recognised qualifications.
20CCP008	The Supplier shall tackle workforce inequality in employment, skills and pay in the contract workforce through supporting in-work progression to help people, including those from disadvantaged or minority groups, to

	move into higher paid work by developing new skills relevant to the contract.
Wellbeing	
20CCP009	The Supplier shall support the health and wellbeing, including physical and mental health, in the contract workforce through offering coaching and resources related to wellbeing.
20CCP010	The Supplier shall encourage collaboration with Users and communities in the codesign and delivery of the contract to support strong integrated communities.
Digital Inclusion	
20CCP011	The Supplier shall support all User segments (Non-digital Users, Low Digitally Skilled Users and Digital Users), including Non-digitally savvy Users who may prefer to seek support through channels such as voice and offline verification.

2.15. Contract Management and Reporting

2.15.1. Contract and Service Management

It will be expected that the Supplier adopts a collaborative approach with the Buyer to ensure both parties fulfil their obligations and the contact centre services are delivered as agreed. These requirements also refer to the need for the Supplier to ensure that the services delivered comply with applicable legal, statutory and regulatory obligations.

ID	Requirement Description
21CCP001	The Supplier shall work collaboratively with the Buyer to ensure both parties fulfil their obligations and the contact centre services are delivered as agreed.
21CCP002	The Supplier shall attend the Operational and Service Review Board (as described in Call Off Special Schedule 8 (Call Off Contract Management)) with the Buyer to review and share: • Recent activity, performance and user support insights • Contact forecasts

	• Any predicted activity which could impact contact volumes • Awareness of any advances in user support contact channels • Change activity and continuous improvement A full agenda will be agreed as part of implementation/transition, along with key milestones and dates.
21CCP003	The Supplier shall attend Quarterly Business Review Board (as described in Call Off Special Schedule 8 (Call Off Contract Management)) with the Buyer to review, share and plan for the new quarter: • Operational planning, including performance reviews for the last quarter • Strategic planning, including development of future features and service journeys that support the Buyer's roadmap • Tactical planning, including defining short-term plans that support the Buyer roadmap • Contingency planning, including outlining plans for unanticipated changes • Executive partnering • Oversight and authority levels • Resolve escalated issues • Cost Saving Report based on evidence A full agenda will be agreed with the Buyer Suppliers Manager prior to these sessions being diarised.
21CCP004	The Supplier will be required to engage with the Buyer Management team/leads on a monthly basis to review, share and plan for following month: • Security Working Group meetings to address risks and support. • Monitor Transition then Service Delivery • Change control

	● Oversee Service Improvement Programme (Transformation and Continuous Improvement) ● Escalation ● Report to Quarterly Business Review Board A full agenda will be agreed with the Buyer Supplier Manager prior to these sessions being diarised.
21CCP005	The Supplier will be required to engage in Operational Meetings with the Buyer on a daily basis to share, review and plan day to day tasks. ● Implement Transition Plan ● Implement service delivery (Service Levels, quality, audits, benchmarking, etc.) ● Change requests ● Recommend new proposals ● Report to Management Committee ● AOB
21CCP006	The Supplier will be expected to travel to the Buyer's operational hub in Manchester, if required for Quarterly Business Review boards to review the contract at a strategic level.
21CCP007	The Supplier shall provide an account management team that will be responsible for delivery of the service. The members of this team, their specific roles and the time allocations for each person should be provided with the tender.
21CCP008	The Supplier shall provide a record and distribute minutes of all board meetings and the actions agreed.
21CCP009	The Supplier shall maintain a service Improvement Log to track and record improvement activity.
21CCP010	The Supplier will have an Ops Leads, Supplier Contract Manager to support in relationship management and operational support and

	additionally the Supplier will suggest how they will support ongoing governance.
21CCP011	The Supplier will have a Supplier Contract manager in line with Call Off Special Schedule 8 (Call Off Contract Management)who is a single point of contact, runs the account management team and will also be responsible for chairing governance meetings as required by the Buyer.
21CCP012	The Supplier must ensure they record, investigate and immediately report to the Buyer any incidents related to any part of their service supporting the Buyer's deliverables. The detailed process is to be agreed with the Buyer.
21CCP013	The Supplier shall agree a process with the Buyer for all Requests for Change where the Supplier's technology and communications solution interfaces to the Buyer's services and systems.
21CCP014	The Supplier shall support the delivery of future changes to GOV.UK One Login Services through requests for change and/or Supplier innovations

2.15.2. Reporting Business Intelligence

The provision of accurate and timely Business Intelligence will be key to ensuring the Supplier Supplier can evidence its performance against the agreed service levels and that the business is meeting their performance targets. A full list of reports that may be required can be found at the Annex to this Schedule, also this in line with '[RM6181 Framework schedule 1 (specification)]'.

ID	Requirement Description
22CCP001	The Supplier shall meet all specified Service Levels as specified in 'Call off Schedule 14 - Service Levels'.
22CCP002	The Supplier shall provide all Business Intelligence (BI) data analysis in Annex A digitally, using advance and customisable Dashboards and other suitable Business Intelligence tools, e.g. Google Analytics and Data Studio

22CCP003	The Supplier shall provide BI reports on an ad hoc basis as requested by the Buyer, adapting their information to suit the individual needs of the Buyer and responding within Service Levels.
22CCP004	The Supplier shall provide a data analysis capability and shall respond to ad hoc requests, such as for cross tabulations and special analysis combining data to identify trends, patterns and clusters based on measurable behaviours, and be able to respond to such requests within 5 Working Days.
22CCP005	The Supplier shall provide an automated feed of raw data which can be integrated with the Buyer's Strategic BI solution, specifically Google Analytics and Data Studio.
22CCP006	The Supplier shall, for each User contact, record and share with the Buyer the reason for the contact using a list of configurable categorisation codes to be agreed with the Buyer.
22CCP007	The Supplier shall share BI data files with the Buyer, so that additional reports can be derived as necessary. These data files must be in a format accessible to the Buyer’s systems and to be agreed with the Buyer .
22CCP008	The Supplier shall work collaboratively with the Buyer , to further determine the exact content and format of the BI reporting to improve reporting and BI.
22CCP009	The Supplier shall provide access to near real time and historical business activity monitoring data, that will allow the Buyer to review the Supplier’s performance against Service Levels as well as establish meaningful data, intelligence and insight into User contacts.
22CCP010	The Supplier shall provide the Buyer with access to view their live contact (chat and call) queue(s), providing information on, but not limited to, the following: ● Agent Availability – telephony and webchat ● Agents In call or chat (total) ● Wrap Up (Agents available but finishing contact notes etc) ● Users in queue (totals waiting by queue)

	● Queue daily performance (Indicates where they are busy)
22CCP011	The Supplier shall provide reports on the top reasons for contact down to a daily level and resolutions to support continuous improvement, chatbot training and contact reduction.
22CCP012	The Supplier shall provide the fully integrated case management capability so that the agents can identify, monitor, manage and resolve Use cases.
22CCP013	The Supplier shall ensure service monitoring events are made available for consumption by the Buyer ' own service monitoring systems.
22CCP014	The Supplier shall provide the tools and run processes to obtain and monitor User feedback, User satisfaction scores across all the contact centre channels. The Supplier will provide weekly reports, in order to improve User support experience and service quality.
22CCP015	The Supplier will provide regular reports on both agent and departmental performance, with the departments having been defined based on the Contact Centre op model.
22CCP016	The Supplier will share a Scope Analysis Report every 3 months that outlines the learnings from the current phase and gives suggestions about potential improvements that the Contact Centre could have in scope. The Scope Analysis Report will determine if additional scope could add value to the User's journey based on analysis and business insights.
22CCP017	The Supplier shall maintain a Cost Savings Log to track and record savings and share Cost Saving Report on quarterly basis during business review, outlining how they propose to drive cost efficiency while delivering a contact centre solution that meets the needs of a wider User segment.

2.16. Implementation and Transition

These requirements refer to the fact that the Contact Centre must be fully operational from the Service Commencement Date. For this to happen there will be a number of tasks undertaken.

ID	Requirement Description

23CCP001	The Supplier shall deliver a fully tested, security assured (as defined by the Buyer's security policy) and operational User Support Contact Centre by October 2023.
23CCP002	The Supplier shall provide a contact management solution along with integration/transition and implementation plan in line with 'Call off Schedule 13 - Implementation Plan and Testing' for the Buyer's approval which includes but is not limited to the below: ● High level implementation plan for evaluation. ● A Security Management Plan to be issued to the Buyer within 20 days of contract agreement between the parties as per Call Off Security Schedule ● Interface Control Documents for each Interface where they have been nominated as the Interface Owner and the Buyer's Change Request documentation. ● Testing Process (as outlined in Call Off Schedule 13). ● All Service Design documentation (any systems/processes being delivered by the service provider which interact with the Buyer or third-party systems or hold or process the Buyer data.) ● Fraud Mitigation Process. ● Any other dependencies including on-going support and management.
23CCP003	The Supplier shall produce an Implementation and Transition Plan detailing how the Supplier will work with the Buyer to outline how it is going to transition from the existing support model to MVP phase 1 . The plan and the associated management of the transition should include consideration of the following areas and be in line with 'RM6181 Framework schedule 1 (specification') ● Preferred approach to implementation and transition for technical systems and business processes ● Key stages for initiation, design, development, testing, data migration, commissioning and transition to full availability and stable operation including a high-level project plan ● How transition to the new service can be successfully and safely carried out to required timescales and target dates

	• Key dependencies on other parties including the Buyer, e.g. any deliverables or information required – including timings, support resource
	• Assumptions and constraints
	• Recruitment onboarding training process
	• Ramp up from cut over (live Day 1) BAU
	• How the plan minimises impact on current services and ensures no disruption to the Identity verification operational business activities and User support
	• How new services will interface with the Buyer's business processes and the order in which they will be deployed
	• What provision is proposed for business continuity during transition and how specific problems will be addressed
	• Identification of implementation and transition risks, and related actions, mitigations and contingencies
	• Approach to reversion / roll-back activities
	• How the service and transition products will be tested and assured
	• The Buyer's Business Change assurance gates
	  ● Information assurance , governance and security
	  ● The Supplier shall be ready to go through the Infrastructure and Projects Buyer (IPA) as required. Gate Review 2 for delivery strategy and/or Gate Review 5 for ops review. Further information about the review toolkit can be found here
	  ● The Suppliers Contract Manager will take the change through the Buyer D3 (Design, Delivery and Decision board).
	• How security of operations and data will be maintained
	• Arrangements for the Buyer to monitor progress
	• Key transition documentation deliverables.
	• Anything else the Supplier feels is needed in the plan.

23CCP004	The Supplier shall work with the Buyer to accept the transfer of any personal User data that may be required and held in the Buyer's systems subject to compliance with the GDPR and the Buyer's security best practices as outlined in Call Off Special Schedule 1 (Security Management).

2.17. Invoicing and Payments

These requirements refer to the invoicing and payments.

ID	Requirement Description
24CCP001	[redacted] [redacted] Buyer's INVOICE ADDRESS: Name: [redacted] [redacted]
24CCP002	Where requested by the Buyer the Supplier shall interface with the Suppliers payment/purchase system as agreed at Call Off stage.
24CCP003	The Supplier must have a solution to accurately account for payments received when delivering the services under the call off contract. These records must be secure and retrievable within 5

	Working Days upon request by the Buyer.
24CCP004	The Supplier shall agree with the Buyer at Call Off stage how to transfer any payments received in delivering the services, but at a minimum the Supplier must have UK based accounting facilities which enable the transfer of funds into an account of the Buyer's choice. Payment shall be transferred daily or at a frequency specified by the Buyer.
24CCP005	The Supplier shall respond to any queries in relation to the remittance for services and/or upon receipt of a reconciliation report from the Buyer within 5 Working Days.
24CCP006	The Supplier shall comply with the Buyer's requirements in respect of authorisation, invoicing and payment processes and procedures.
24CCP007	Invoices shall be created in line with the Buyer's requirements but at a minimum they must contain itemised charges for service provided and rates applied.

Annex to Call Off Special Schedule 2 - Business Intelligence and Insights in Real Time

1	**The Contractor will provide Business Intelligence for User contacts**	Daily summaries and in real time of performance to include, but not be limited to: 1. Channel mix – total contacts handled by each channel with % split 2. Cost per contact, per channel 3. Average handling time per channel 4. Average Time To Answer per channel 5. Answer Rate – call and chat

		6. Average speed of response – all channels 7. Number of chatbot conversations 8. Number of chatbot conversations contained 9. Chatbot containment rate 10. Average CSAT scores per channel 11. Total number of complaints received 12. Total number of complaints closed 13. “Right first time” report
		Weekly summaries of performance as above, plus: 1. Dropped contacts a) At IVR stage i. Actual ii. As a percentage b) At connection – voice, chatbot, webchat i. Actual ii. As a percentage c) During connected stage for agent-handled call or webchat i. Actual ii. As a percentage 2. Inbound contacts total by hour, by channel 3. Chatbot containment rate 4. Top 10 reasons for contact by channel

		5. “Right first time” tracker
		As above for calendar month, 4 weekly cycle, quarterly and annual plus : 1. Details of call types based on both IVR/contextual voice routing and agent- categorised call purpose 2. Repeat calls 3. CSAT scores overall 4. CSAT scores by call type
		A record of the reason for the contact
		A record of all outbound emails in a retrievable format.
		Country based information for international Users
2	**The Contractor will provide business intelligence for the GOV.UK** **One Login Platform**	Breakdown of types User using the GOV.UK One Login platform service
		Breakdown of outcomes- Verified/Not Verified/ Referral
		Total calls received
		Total calls abandoned before answering
		Call wait times
		Total number of emails received, answered and pending
3	**The Contractor will provide business intelligence for fraud risks and threats.**	1. Threat intelligence relevant to the Contractor’s organisation and function.

4	**The Contractor will provide will provide business intelligence for the contact centre staff**	1. ENPS 2. Absenteeism 3. Shrinkage
5	**The Contractor shall be required to report on the performance and delivery of the contract. RM6181 Framework schedule 1 (specification)**	1. Summary of charges, credits and forecast; 2. Detailed periodic performance against Service Levels 3. Users insight (including complaints); 4. Availability, utilisation and use of systems; 5. Performance of support services such as Contact Centres; 6. Sub-Contractor performance or performance against any Operating Level; 7. Agreements (SLAs); 8. Reporting on contract change and work orders, including of their delivery; and 9. Continuous improvement.

Call Off Special Schedule 3 – Supplier Solution

[redacted]

PHASE – ONE

[redacted]

User Experience

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Functional Requirements that can't be met

[redacted]

Assumptions

[redacted]

Dependencies

[redacted]

Manage, Train, Retain Staff to ensure Continuity/Quality

[redacted]

Resource Planning

[redacted]

Recruitment

[redacted]

Training

[redacted]

[redacted]

Quality/Performance

[redacted]

IMAGE REDACTED

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

Retaining Staff

[redacted]

PHASE-TWO

[redacted]

IMAGE REDACTED

User Experience

[redacted]

IMAGE REDACTED

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Functional Requirements that can’t be met

[redacted]

[redacted]

Assumptions

[redacted]

Dependencies

[redacted]

Manage, Train, Retain Staff to ensure Continuity/Quality

Resourcing

[redacted]

Recruitment

[redacted]

Training

[redacted]

Performance/Quality

[redacted]

Retaining Staff

[redacted]

Solution Technologies

[redacted]

[redacted]

PROPOSED SOLUTION

[redacted]

[redacted]

[redacted]

TECHNOLOGIES DEPLOYED

[redacted]

[redacted]

Integrations Required

[redacted]

Reliance and Support from the Authority

[redacted]

[redacted]

[redacted]

HARDWARE

[redacted]

Dedicated Telephony

[redacted]

IT Hosting/Architecture

[redacted]

IMAGE REDACTED

Essential upgrades

[redacted]

OMNI-CHANNEL SERVICES

[redacted]

IMAGE REDACTED

Telephony/Webchat

[redacted]

Email/RPA

[redacted]

Chatbot

[redacted]

Knowledgebase

[redacted]

Speech/Interaction Analytics

[redacted]

CRM

[redacted]

Call Off Special Schedule 4 – Continuous Improvement

1. Buyer's Rights

1.1 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.

2. Supplier's Obligations

2.1 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.

2.2 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.

2.3 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:

2.3.1 identifying the emergence of relevant new and evolving technologies;

2.3.2 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);

2.3.3 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

2.3.4 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.

2.4 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.

2.5 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.

2.6 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.

2.7 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.

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

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

2.8.2 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.

2.9 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.

2.10 [redacted]

2.11 Subject to paragraph 2.12 below, 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.

2.12 [redacted]

2.12.1 [redacted]

[redacted]

2.12.2 [redacted]

(a) [redacted]

(b) [redacted]

2.12.3 [redacted]

Call Off Special Schedule 5 – Implementation Plan and Testing

Part A - Implementation

1. Definitions

1.1 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;
[redacted]	[redacted]
"Delay Payment Limit"	[redacted]
"Delay Period Limit"	means the number of days the delay exceeds the agreed upon date that is specified in the implementation plan
"Deliverable"	an item, artefact or feature to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan. For the avoidance of doubt, a set of deliverable items can make up a Milestone;
"Milestone"	Events and/or tasks described under in the Annex 1 Implementation Plan which, if applicable, must be completed by the relevant Timeframe

	or Delivery Date. For the avoidance of doubt, a set of deliverable items can make up a Milestone;
"Milestone Payment"	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"	has the meaning given to it in Paragraph 7.1;
“Milestone Achievement ”	a milestone that has been achieved and has been approved by the Buyer by the issue of a Satisfaction Certificate;

2. Agreeing and following the Implementation Plan

2.1 A draft of the Implementation Plan is set out in the Annex to this Schedule. The Supplier shall provide a further draft Implementation Plan twenty (20) days after the Call-Off Start Date.

2.2 The draft Implementation Plan:

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

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

2.3 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 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.

2.4 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.

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

3. Reviewing and changing the Implementation Plan

3.1 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.

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

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

3.4 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.

4. Security requirements before the Start Date

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

5. What to do if there is a Delay

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

5.1.1 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;

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

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

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

6. Compensation for a Delay

6.1 [redacted]

6.1.1 [redacted]

6.1.2 [redacted]

(a) [redacted]

(b) [redacted]

6.1.3 [redacted]

6.1.4 [redacted]

6.1.5 [redacted]

6.1.6 Not used.

6.1.7 [redacted]

6.1.8 [redacted]

Late Delivery of Deliverables

6.2 The Supplier shall deliver the agreed Deliverables by the timeframe or delivery dates (outlined in Annex 1: Implementation Plan), subject to any mutually agreed extensions.

6.3 Not used.

6.4 Not used.

6.5 If the delay of the Deliverable exceeds the maximum of 5 Working Days, the Supplier may submit a request to the Buyer for a meeting to discuss a resolution plan. The Buyer shall respond to the request within 2 Working Days of receipt of the request. The Supplier and Buyer shall work together in good faith to develop a resolution plan to mitigate the delay, and any costs associated with implementing the resolution plan shall be borne by the party responsible for the delay.

6.6 If the parties are unable to reach a resolution plan within 10 Working Days, the Buyer retains the right without prejudice to terminate this Contract and/or claim damages from the Supplier for material Default.

7. Implementation Plan

7.1 The Implementation Period will be a three (3) Month period from the Call-Off Start Date.

7.2 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.

7.3 In accordance with the Implementation Plan, the Supplier shall:

7.3.1 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;

7.3.2 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;

7.3.3 liaise with the incumbent Supplier to enable the full completion of the Implementation Period activities; and

7.3.4 produce an Implementation Plan, to be agreed by the Buyer, for carrying out the requirements within the Implementation Period including, key Milestones and dependencies.

7.4 The Implementation Plan will include detail stating:

7.4.1 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

7.4.2 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.

7.5 In addition, the Supplier shall:

7.5.1 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;

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

7.5.3 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:

(a) 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

(b) 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.

7.5.4 manage and report progress against the Implementation Plan;

7.5.5 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;

7.5.6 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

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

Annex 1: Implementation Plan

The Deliverables and Milestones will be Achieved in accordance with this Schedule.

Unless the parties agree otherwise, the delivery of documentation in the table below within the relevant timeframe or by the relevant delivery date refers to the delivery of draft documentation by the Supplier along with an agreed process for joint completion and approvals.

For the purposes of Paragraph 6.1.2 the Delay Period Limit shall be 10 Working Days.

The Implementation Plan is set out below and includes Milestones and Deliverables the Supplier is required to Achieve:

Deliverable Items	**Description**	**Timeframe or Delivery Date**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted] 23CCP002)	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Deliverable Items	Description	Timeframe or Delivery Date
		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Deliverable Items	Description	Timeframe or Delivery Date
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Milestones: Phase 1		**Time frame or Delivery Date**	**Delay Payments**
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
Milestones: Future Phases (2-3)			
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

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

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"	any constituent parts of the Deliverables;
"Material Test Issue"	a Test Issue of Severity Level 1 or Severity Level 2;
"Satisfaction Certificate"	a certificate materially in the form of the document contained in Annex 2 to Part B issued by the Buyer when a Deliverable and/or Milestone has satisfied its relevant Test Success Criteria;
"Severity Level"	the level of severity of a Test Issue, the criteria for which are described in Annex 1 to Part B;
"Test Issue Management Log"	a log for the recording of Test Issues as described further in Paragraph 8.1 of this Schedule;
[redacted]	[redacted]
"Test Reports"	the reports to be produced by the Supplier setting out the results of Tests;
"Test Specification"	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;
"Test Strategy"	a strategy for the conduct of Testing as described further in Paragraph 3.2 of this Schedule;

"Test Success Criteria"	in relation to a Test, the test success criteria for that Test as referred to in Paragraph 5 of this Schedule;
"Test Witness"	any person appointed by the Buyer pursuant to Paragraph 9 of this Schedule; and
"Testing Procedures"	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.

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

4.2.2 a 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 and approved

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.

6.3 The Deliverable shall be deemed to have been delivered on the date that the Buyer confirms in writing that the Deliverable meets the Buyer's requirements.

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.

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 [redacted]

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 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.

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).

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.

Annex 1 to Part B: Test Issues – Severity Levels

1. Severity 1 Error

1.1 [redacted]

2. Severity 2 Error

2.1 [redacted]

2.1.1 [redacted]

2.1.2 [redacted]

2.1.3 [redacted]

3. Severity 3 Error

3.1 [redacted]

3.1.1 [redacted]

3.1.2 [redacted]

3.1.3 [redacted]

[redacted]

4. Severity 4 Error

4.1 [redacted]

5. Severity 5 Error

5.1 [redacted]

Annex 2 to Part B: Satisfaction Certificate

To: [insert name of Supplier]

From: [insert name of Buyer]

[insert Date dd/mm/yyyy]

To whom it may concern

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 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 Special Schedule 6 – Service Levels

1. Definitions

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

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

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

1.2 [redacted]

2. What happens if you don't meet the Service Levels

2.1 [redacted]

2.2 [redacted]

2.3 [redacted]

2.4 [redacted]

2.4.1 [redacted]

2.4.2 [redacted]

(a) [redacted]

(b) [redacted]

(c) [redacted]

(d) [redacted]

2.4.3 [redacted]

2.5 [redacted]

2.5.1 [redacted]

2.5.2 [redacted]

2.5.3 [redacted]

2.6 [redacted]

2.6.1 [redacted]

2.6.2 [redacted]

a) [redacted]

b) [redacted]

c) [redacted]

3. Critical Service Level Failure

[redacted]

3.1 [redacted]

3.2 [redacted]

Part A: Service Levels and Service Credits

1. Service Levels

[redacted]

1.1 [redacted]

1.2 [redacted]

[redacted]

1.2.1 [redacted]

1.2.2 [redacted]

1.2.3 [redacted]

1.2.4 [redacted]

2. Service Credits

2.1 [redacted]

2.2 [redacted]

3. Annual Increase of Key Service Level Performance Measures

3.1 [redacted]

[redacted]

[redacted]

4. Service Bonus Structure

4.1 [redacted]

Worked Example:

[redacted]

[redacted]

4.2 Annex A to Part A: Service Levels and Service Credits Table

Table 1 - User Experience Service Levels

LOT 1 User Experience Service Levels				Service Credits	Service Bonus
Service Level Performance Criterion	**Service Level Performance Measure**	**Service Level Performance Definition**	**Measurement Period**	**Service Credit Applied**	**Service Bonus Potential**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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

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

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

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

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

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

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

[redacted]

[redacted]

		[redacted]			

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

[redacted]

		[redacted]			

Table 2 Business Area or Service Line Specific Service		Service Credits	Service Bonus
Table 2 below illustrates Service Levels Business Area Specific as they apply only to a particular Business Area, or Service Line(s) or Contact Channel(s) within a particular Business Area based on unique business requirements.			

Service Level Performance Criterion	Service Level Performance Measure	Service Level Performance Definition	Measurement Period	Service Credit Applied	Service Bonus Potential
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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

[redacted]		[redacted]			

		As soon as practicable following the Start Date and in any event prior to service go-live.			

		(a) the Operational and Service Review Board forum will be used by the parties to understand and agree measurement of the above and any applicable Service Credits; and			

Annex B to Part A: Service Level Thresholds and Service Credit Points

Service Levels				Service Credit Points for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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

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

[redacted]

[redacted]

Table 2 Business Area or Service Line Specific Service				
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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

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

[redacted]

Service Credit Calculation

[redacted]

[redacted]

Part B: Performance Monitoring

5. Performance Monitoring and Performance Review

5.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

5.2 The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the process and timescales agreed pursuant to paragraph 3.1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

5.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

5.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;

5.2.3 details of any Critical Service Level Failures;

5.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

5.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and

5.2.6 such other details as the Buyer may reasonably require from time to time.

5.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

5.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;

5.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and

5.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.

5.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.

5.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

6. Satisfaction Surveys

6.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the satisfaction surveys reasonably suggest are not in accordance with this Contract.

Call Off Special Schedule 7 – Pricing Details

[redacted]

1. Charges for this Call-Off Contract

[redacted]

[redacted]

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

[redacted]

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

[redacted]

IMAGE REDACTED

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

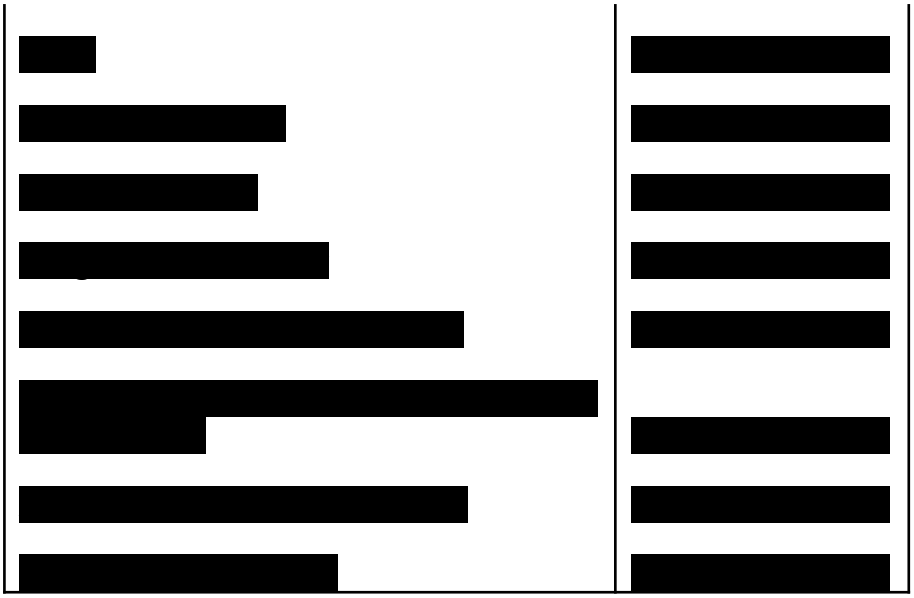
[redacted]

[redacted]

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

Rate Card

Role	Day Rate
[redacted]	[redacted]



Price Workbooks 4a/4b/4c

[redacted]

FILE REDACTED

[redacted]

FILE REDACTED

[redacted]

FILE REDACTED

2. Volume Variations and Costing Adjustments

2.1 [redacted]

2.2 [redacted]

1. [redacted]

2. [redacted]

3. [redacted]
4. [redacted]
    1. [redacted]
    2. [redacted]
    3. [redacted]
5. [redacted]

2.3 [redacted]

Call Off Special Schedule 8 – 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):

"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

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. Contract Boards

4.1 The Parties shall establish and operate the boards and groups set out in the Annex to this Schedule (being the "**Contract Boards**").

4.2 In the event that either Party wishes to replace any of its appointed Contract 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.

4.3 Each Party shall ensure that its Contract 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 Contract 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.

4.4 Minutes shall be recorded for each Contract Board meeting, capturing the key decisions, action items, and any other relevant information. The Supplier shall provide the minutes to the Buyer within 48 hours . In addition, the Supplier shall prepare periodic reports summarising the outcomes and progress made during the Contract Board meetings.

4.5 The effectiveness and relevance of the Contract Boards shall be reviewed periodically by the Parties. If necessary, modifications to the composition, frequency, or scope of the boards may be proposed and mutually agreed upon in writing by the Parties.

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;

5.2.3 monitoring and controlling project plans; and

5.2.4 monitoring and disclosing to the Buyer any risks allocated by the Supplier to their supply chain.

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.

Annex: Contract Boards

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

A. Quarterly Business Review Board

Purpose	Established as an executive steering committee to facilitate executive partnering, provide oversight and authority levels, drive strategic planning, and efficiently resolve escalated issues.
Start date	Buyer to notify
Frequency	Quarterly
Location	Buyer to notify
Attendees	Parties to agree

B. Operational and Service Review Board

Purpose	Review the Supplier's performance under this Contract, forecasts (including a locked 4-week and 9-month view), as well as Service Levels and Key Performance Indicators. Additionally, every other board session shall be extended to cover contract management topics, such as change requests. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.
Start date	Buyer to notify
Frequency	Fortnightly
Location	Buyer to notify
Attendees	Parties to agree

C. Working Group

Purpose	During the implementation and transition phases, provide regular updates on project progress, risks, and issues. The Working Group shall also collaborate on requirements and design options/decisions.
Start date	Buyer to notify

Frequency	Weekly
Location	Buyer to notify
Attendees	Parties to agree

D. Transition Board

Purpose	Provide strategic direction and oversight of the transition process. The Transition Board shall also approve key deliverables related to the transition.
Start date	Buyer to notify
Frequency	Fortnightly
Location	Buyer to notify
Attendees	Parties to agree

Call Off Special Schedule 9 – 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
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

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

	[redacted]	[redacted]	