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

Order Form

CALL-OFF REFERENCE:	con_23861 Third Party Identification Verification Services
THE BUYER:	Office of Public Guardian (OPG) as Executive Agency sponsored by **The Secretary of State for Justice acting through the Ministry of Justice.**
BUYER ADDRESS:	Victoria Square House, 1 Pinfold Street, Birmingham, B2 4AA
THE SUPPLIER:	Experian Ltd
SUPPLIER ADDRESS:	The Sir John Peace Building Experian Way, NG2 Business Park, Nottingham, NG80 1ZZ
REGISTRATION NUMBER:	653331

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 14 December 2021.

It's issued under the Framework Contract with the reference number RM6226 for the provision of Third-Party Verification Services

CALL-OFF LOT(S):
2- Data Solutions of the Debt Resolution Service

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract[1]. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM6226
3. Framework Special Terms
4. The following Schedules in equal order of precedence:

- Joint Schedules for Framework Contract RM6226
    - Joint Schedule 2 (Variation Form and Change Control Procedure)
    - Joint Schedule 3 (Insurance Requirements)
    - Joint Schedule 4 (Commercially Sensitive Information)
    - Joint Schedule 10 (Rectification Plan)
    - Joint Schedule 11 (Processing Data)

- Call-Off Schedules for con 23861
    - Call-Off Schedule 1 (Transparency Reports)
    - Call-Off Schedule 2 (Staff Transfer)
    - Call-Off Schedule 3 (Continuous Improvement)
    - Call-Off Schedule 5 (Pricing Details)
    - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
    - Call-Off Schedule 9 (Security Requirements)
    - Call-Off Schedule 13 (Implementation Plan and Testing)
    - Call-Off Schedule 15 (Call-Off Contract Management)
    - Call-Off Schedule 20 (Call-Off Specification - including Appendix - Experian's Service Description.

[1] Only schedules that have been amended from the standard CCS terms and conditions have been included. These are Joint Schedule 11 (Processing Data), Call-Off Schedule 5 (Pricing Details) and Call-Off Schedule 9 (Security Requirements). The other Schedules listed still apply in the order of precedence stated.

- CCS Core Terms (version 3.0.11)

5. Joint Schedule 5 (Corporate Social Responsibility) RM6226

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 – See Appendix 1 - Table of Amendments for Experian Ltd required Special Terms and Conditions.
Appendix 2 - Experian Required Special Terms and Conditions (agreed amended) 1. Fraudscore, 2. Identity Authenticate 3. Royal Mail NCO Alert Data – End User Agreement, 4. Experian Data Quality Addendum, and 5. Experian Terms and Conditions Version 5.

Special Term 2. The Framework Terms and Conditions and Call-Off Incorporated Terms in regards to this call-off will take precedence over the Special Term 1 (Experian's additional Terms and conditions).
For the avoidance of doubt Experian's Amended Additional Terms and Conditions will sit at number 6 in the order of precedence after Joint Schedule 5.

Special Term 3. Charges for transactions – for each OPG check being either an ID, KBV and/or Fraud, are each an individual transaction and will be charged as 1 (one) individual transaction. – Reference Call-Off Schedule 5

It is noted that the Call-Off Order Form is being signed on the basis that information outstanding in Call-Off Schedule 9 – Security Requirements – Appendix 1 and Appendix 2 are provided by Experian within 30 days of the Call-Off Start Date listed below.

CALL-OFF START DATE: **28th June 2024**

CALL-OFF EXPIRY DATE: **28th June 2027**

CALL-OFF INITIAL PERIOD: **3 Years**

CALL-OFF OPTIONAL EXTENSION PERIOD **1 x 12 months**

CALL-OFF DELIVERABLES

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

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

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **£115,250.00**

CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details)
All changes to the Charges must use procedures that are equivalent to those (if used) in Framework Schedule 3 (Framework Prices)]

REIMBURSABLE EXPENSES
None

PAYMENT METHOD
The payment method for this Call-Off Contract is BACS

Payment Terms: Settlement is due within 30 days of invoice date.

BUYER'S INVOICE ADDRESS:
[REDACTED]

BUYER'S AUTHORISED REPRESENTATIVE
[REDACTED]

BUYER'S ENVIRONMENTAL POLICY
Documents are available at: Climate change and environmental sustainability: MOJ - GOV.UK (www.gov.uk)

BUYER'S SECURITY POLICY
Contractors providing goods or services to the Ministry of Justice are bound by the Official Secrets Acts 1911 to 1989. The 1989 Act makes it an offence for any person employed by a government contractor to disclose any document or information which is likely to result in the commission of an offence or facilitate an escape from legal custody or the doing of any other act prejudicial to the safekeeping of persons in legal custody.
The contractor's Staff will also be subject to a general obligation of confidentiality in respect of information acquired through providing the Services and will be required to sign a Confidentiality Undertaking.
The Ministry of Justice will also exercise the right usually given in government contracts, requiring the contractor to identify all members of his staff who will be involved in fulfilling the contract. The contractor may be required to supply other information the Ministry of Justice may require for determining whether there is any objection to a particular member of his staff being admitted to Ministry of Justice premises. The Ministry of Justice will have the right to exclude any person specified by the Ministry of Justice from those premises.
All contractors would be required to comply with the statements set out above.

SUPPLIER'S AUTHORISED REPRESENTATIVE
[REDACTED]

PROGRESS REPORT FREQUENCY
Monthly Management Information (MI) and Key Performance Indicators (KPI) reporting.

PROGRESS MEETING FREQUENCY
Monthly Performance Review meeting
Quarterly Strategic Review meeting

KEY STAFF
[REDACTED]

KEY SUBCONTRACTOR(S)
NA

COMMERCIALLY SENSITIVE INFORMATION
Not applicable

SERVICE CREDITS
Not applicable

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT
Not applicable to this Call-Off contract but is applicable to the Framework – CCS manages.

Call-Off Schedule 9 (Security Requirement)

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

Appendix 1 – Amended Terms and Conditions **Special Terms & Conditions**

1.1 **FRAUDSCORE SPECIFIC TERMS**

1.2

Definition	**Meaning**
"Application Data"	means the data in the applications received by the Client from individuals to purchase goods and/or services from the Client

1. The Fraudscore Service is based on the use of machine learning and automated intelligence statistical techniques ("AI Techniques") that analyse the Application Data submitted by a consumer to acquire a Client's product. The Application Data is computed through a machine learning (ML) model which is trained on a given date and is not self-learning. The service returns a fraud propensity score (0-1000) and, where requested, a list of reason codes which will help explain the score. The Client acknowledges that Experian doesn't warrant the accuracy and quality of the score returned nor does Experian accept any liability in the event of inaccurate decisioning made by the Client due to their over-reliance on the services in their fraud strategies resulting in reputational risk or financial loss
2. The Client is solely responsible for ensuring their automated rejection rate does not exceed 5% of all applications or transactions. If the rejection rate does increase beyond 5%, The Client is solely responsible for informing Experian and requesting adjustments to their rejection threshold.
3. The Client is solely responsible for determining the identity, suitability, personal details and creditworthiness of any User that makes an application for any of the Client's Products and acknowledges that none of the information which Experian provides to the Client in respect of any User is intended to be relied solely upon by the Client for credit reference, authentication or fraud prevention purposes;
4. The Client acknowledges that the FraudScore Service will process personal data that is submitted into the Service by the Client, including any belonging to minors or vulnerable individuals. As a data controller under GDPR, and without prejudice to the Client's obligations under Clause 18.1 of the Terms and Conditions, the Client will ensure that it has appropriate controls and measures in place within the Client systems and processes to satisfy the requirements of the GDPR in relation to any individuals. The Client shall ensure that their

privacy policy to their consumers includes a notification of the use of the services for the prevention and detection of crime/fraud.

Definition	Meaning
"Batch"	means a mechanism representing a service which allows the transfer of an Initial Input File provided by the Client via Secure Transfer Protocol (STS), in the format specified within the template provided by Experian to the Client, and the return by Experian of an output file with the processed data via the same process.
"CrossCore Transaction"	means a transaction submitted via the CrossCore Submit API to access one or multiple Services with a corresponding response via the Client Response API. Refer to the CrossCore Swagger document listed in the Specification section above for further detail.
"Experian CrossCore" or "CrossCore"	means Experian's on-demand, web-based platform and decisioning tool for fraud and identity verification assessment, transaction viewing, workflows and reporting, which incorporates, as applicable, the Services listed in Section 1
"Project Plan"	means a formal approved document used to guide both project execution and project control. It details key tasks and milestones with associated resource allocations and durations
"**UI"** or "**User Interface"**	means a web page hosted by Experian within the Experian infrastructure
"**User**"	means an individual or application who has access to CrossCore either via UI or Web Service
"Web Service"	means a JSON based service for communications between the Client's business applications and CrossCore

Call-Off Schedule 9 (Security Requirement)

Crown Copyright 2021

'JSON'	JSON (JavaScript Object Notation) is a lightweight, open standard, data-interchange format using human-readable text to transmit data objects consisting of attribute-value pairs in machine-readable form and is used in the development of the Web Service (as opposed to the User Interface)

USE OF DATA, PRODUCT ENHANCEMENTS AND IMPROVEMENTS

1. The Client hereby grants Experian the right to use Client Data sent to Experian for storage and/or processing through CrossCore in accordance with its provision of the applicable Experian Service(s) to the Client.
2. The Client further agrees to provide Experian application outcome feedback on a monthly basis during the Term based on its use of the Experian Service(s) ("Outcome Reporting") in the format specified by Experian or as otherwise agreed by the parties in writing.
3. The Client grants Experian the right to use Client Data and Outcome Reporting for validation, deployment, measurement, improvement, research, development and optimisation of CrossCore and the Experian Service(s). The Client acknowledges that Experian may incorporate these developments, improvements and performance optimizations into and for use within Experian's Identity and Fraud services generally, including the validation, deployment, measurement, improvement, research, development and/or optimisation of generic machine learning models. Unless otherwise agreed with the Client, no Outcome Reporting or Client Data will be disclosed to Experian's clients.

CLIENT OBLIGATIONS

4. The Client shall ensure that it maintains reasonable anti-virus and data security controls.
5. The Client is responsible for all activities of its Users.

UPDATES

6. Experian may release Updates, which may modify CrossCore and the Services, from time-to-time ("Updates"). Experian agrees that it will use reasonable endeavours to ensure that such Updates will not result in a material reduction in the level of performance or availability or functionality of CrossCore or the latest version of Experian Service(s) provided to the Client through CrossCore. Updates will be subject to this Agreement.
7. If Experian is aware that implementing an Update will result in a material reduction in or unavailability either of CrossCore or any of the Services the Client is currently using, Experian will make commercially reasonable efforts to notify the Client ninety (90) days before the required implementation of the relevant Update.

Call-Off Schedule 9 (Security Requirement)

Crown Copyright 2021

SUPPLIER TERMS AND CONDITIONS FOR THE PROVISION OF PRODUCTS AND SERVICES –IDENTITY AUTHENTICATE ("SUPPLIER TERMS AND CONDITIONS")

SUPPLIER TERMS AND CONDITIONS PART A

SERVICE SPECIFIC TERMS

SERVICE AND SUPPORT TERMS
The Supplier shall provide the Services in accordance with the Supplier Terms and Conditions Part C (Service and Support Terms).

Definition	Meaning
"Batch"	means a mechanism representing a service which allows the transfer of an Initial Input File provided by the Client via Secure Transfer Protocol (STS), in the format specified within the template provided by Experian to the Client, and the return by Experian of an output file with the processed data via the same process.
"CrossCore Transaction"	means a transaction submitted via the CrossCore Submit API to access one or multiple Services with a corresponding response via the Client Response API. Refer to the CrossCore Swagger document listed in the Specification section above for further detail.
"Experian CrossCore" or "CrossCore"	means Experian's on-demand, web-based platform and decisioning tool for fraud and identity verification assessment, transaction viewing, workflows and reporting, which incorporates, as applicable, the Services listed in Section 1
"Project Plan"	means a formal approved document used to guide both project execution and project control.

	It details key tasks and milestones with associated resource allocations and durations
"**UI"** or "**User Interface"**	means a web page hosted by Experian within the Experian infrastructure
"**User**"	means an individual or application who has access to CrossCore either via UI or Web Service
"Web Service"	means a JSON based service for communications between the Client's business applications and CrossCore
'JSON'	JSON (JavaScript Object Notation) is a lightweight, open standard, data-interchange format using human-readable text to transmit data objects consisting of attribute-value pairs in machine-readable form and is used in the development of the Web Service (as opposed to the User Interface)

USE OF DATA, PRODUCT ENHANCEMENTS AND IMPROVEMENTS

8. The Client hereby grants Experian the right to use Client Data sent to Experian for storage and/or processing through CrossCore in accordance with its provision of the applicable Experian Service(s) to the Client.
9. The Client further agrees to provide Experian application outcome feedback on a monthly basis during the Term based on its use of the Experian Service(s) ("Outcome Reporting") in the format specified by Experian or as otherwise agreed by the parties in writing.
10. The Client grants Experian the right to use Client Data and Outcome Reporting for validation, deployment, measurement, improvement, research, development and optimisation of CrossCore and the Experian Service(s). The Client acknowledges that Experian may incorporate these developments, improvements and performance optimizations into and for use within Experian's Identity and Fraud services generally, including the validation, deployment, measurement, improvement, research, development and/or optimisation of generic machine learning models. Unless otherwise agreed with the Client, no Outcome Reporting or Client Data will be disclosed to Experian's clients.

CLIENT OBLIGATIONS

11. The Client shall ensure that it maintains reasonable anti-virus and data security controls.
12. The Client is responsible for all activities of its Users.

UPDATES

13. Experian may release Updates, which may modify CrossCore and the Services, from time-to-time ("Updates"). Experian agrees that it will use reasonable endeavours to ensure that such Updates will not result in a material reduction in the level of performance or availability or functionality of CrossCore or the latest version of Experian Service(s) provided to the Client through CrossCore. Updates will be subject to this Agreement.

14. If Experian is aware that implementing an Update will result in a material reduction in or unavailability either of CrossCore or any of the Services the Client is currently using, Experian will make commercially reasonable efforts to notify the Client ninety (90) days before the required implementation of the relevant Update.

15.

PERMITTED PURPOSE
If the Services include International Identify Verification and/or Identity Authenticate and/or CrossCore Identity Services for UK KYC the Permitted Purpose will be limited to use for the purposes of identity verification, date of birth verification and to assist in preventing money laundering only

IDENTITY AUTHENTICATE

1. The Buyer will ensure that at the point of collection of the personal data, the relevant individual is informed of the following principles;

   - A search will be carried out with the Supplier for the purposes of verifying their identity.
   - The Supplier may check the details they supply against any particulars on any database (public or otherwise) to which they (the Supplier) have access in order to verify their identity.
   - The Supplier will retain a record of the search.

2. If any such notification is not provided by the Buyer, the Buyer undertakes to the Supplier that it shall not attempt to use the Supplier Services in respect of the relevant individual.
3. If the Buyer is taking any Services utilizing Royal Mail NCOA® Alert Data, the provisions of Appendix 1 to this Supplier Terms and Conditions Part A entitled "Royal Mail NCOA® Alert Data - End User Agreement" shall apply.
4. In order for the Supplier to provide the Services to the Buyer and in order for the Supplier to comply with the licence terms which British Telecommunications plc and/or other third party suppliers of telephone number data require, all users of such data similar to the Supplier shall be required to accept the following:
   4.1 The Buyer
      4.1.1 appoints the Supplier as its agent under this Agreement for the purpose of using Buyer Data to carry out directory enquiry searches for and on behalf of the Buyer;

4.1.2 authorises and instructs the Supplier to:

4.1.2.1 use any retrieved telephone numbers resulting from such directory enquiries for the sole purpose of comparing such telephone numbers against any telephone numbers contained within the relevant and applicable Buyer Data and producing a score based upon whether there was or was not a match of telephone numbers; and

4.1.2.2 incorporate the score referred to in paragraph 4.1.2.1 into the overall score delivered to the Buyer by the Services; and

4.1.3 instructs and confirms to the Supplier that telephone numbers retrieved from such directory enquiry searches are for use as input into the comparison process described in paragraph 4.1.2.1 only and the Supplier is not required to return such telephone numbers to the Buyer.

5. The Buyer acknowledges that where the Buyer is licensed to access GRO Mortality data within the Supplier Services the Buyer must provide, as a minimum, name and date of birth details for the relevant individual.

Appendix 1 (applicable to all services except Experian Data Quality services)

Royal Mail NCOA® Alert Data – End User Agreement

The Royal Mail has stipulated that the following terms and conditions shall apply to a Buyer of the Supplier who is licensed to receive Royal Mail NCOA® Alert Data. These terms and conditions have been imposed by Royal Mail and the Supplier has no authority or ability to agree any amendments. In this End User Agreement, references to "the End User" are references to the Buyer, references to "the Licensee" are references to the Supplier, references to "this Agreement" are to this End User Agreement and/or to the use of Royal Mail NCOA® Alert Data within the Services (as the context requires) and the following terms have the following meanings:

- Definitions

"Applicant"	an applicant for the End User's products or services;
"Applicant Record"	the name and address (and, where available, the date of birth) of an Applicant which have been lawfully and fairly obtained by the End User for the purpose of verifying the Applicant's application for the relevant product or service of the End User;

"DPA"	the Data Protection Act 1998;
"EEA"	the European Economic Area comprising, for the time being, the EU member states, Norway, Iceland and Liechtenstein;
"Intellectual Property Rights"	all intellectual property rights including copyright and related rights, database rights, trade marks and trade names, patents, topography rights, design rights, trade secrets, know-how, and all rights of a similar nature or having similar effect which subsist anywhere in the world, whether or not any of them are registered and applications for registrations, extensions and renewals of any of them;
"Match"	each instance where any of the name and address (and, where available, the date of birth) fields within an Applicant Record is identified as the same as or is an abbreviation, extension or variation of the full name and Old Address (and, where available, the date of birth) fields included in the NCOA® Alert Data;
"NCOA ® Alert Data"	the Redirection Data and Non-Redirection Data licensed to the Licensee by Royal Mail which is comprised in the Product and shared with the End User by way of an Output;
"New Address"	the address specified by a Redirection Customer as that to which mail should be redirected (as subsequently amended by Royal Mail, if necessary, to ensure that the address information is correct for Royal Mail's postal purposes);
"Non-Redirection Data"	data collected from databases or sources other than the Redirection Forms;
"Old Address"	the address specified by a Redirection Customer as that from which mail should be redirected (as subsequently amended by Royal Mail, if necessary,
"Outputs"	the elements of the NCOA® Alert Data which shall be provided to the End User in the case of a Match;
"Permitted Purpose "	to search for and identify Matches in order to find out where a mail redirection is or has been in place or is pending in the name of an Applicant for the explicit purpose of verifying the identity of the Applicant for the prevention

	of fraud including cases of money laundering and impersonation of the Applicant;
"Product"	any product, service or other solution which is modified or enhanced by, incorporated with, created using, derived from or involves the supply or the making available of, the Outputs;
"Redirection Customer"	a customer of the Redirection Service;
"Redirection Data"	data collected from the Redirection Forms completed by Redirection Customers;
"Redirection Form"	the application form completed by individuals who wish to use the Redirection Service;
"Redirection Service"	Royal Mail's redirection service provided to members of the public who wish to have mail which is addressed to them forwarded from their old address to their new address;

Licence

- In consideration of the End User complying with these Minimum Terms, the Licensee grants to the End User a non-exclusive, non-transferable, revocable sub-licence to access and use the NCOA® Alert Data accessed as part of its use of the Product in the EEA only for the Permitted Purpose.
- The End User shall not at any time, sell, deal, transfer, sub-license, distribute, commercially exploit, or otherwise make available to third parties or use for the benefit of third parties the whole or any part of the NCOA® Alert Data other than in accordance with these Minimum Terms.
- The End User shall not copy, adapt, alter, modify, or otherwise interfere with the Outputs or combine the same with other materials or data.
- The End User shall not assign, sub-contract or otherwise deal with the End User Agreement or any part of it.
- The End User shall be permitted to search for Matches either in respect of individual Applicants or a batch of Applicants at the same time.
- The End User shall not retain any Outputs and/ or information relating to Matches on Applicant Records or credit files, provided that, by way of exception and where relevant, the End User may separately retain information on Matches only for a period of up to a maximum of five years from the date of termination of the relevant customer relationship in so far as and for as long as this is necessary to comply with the Financial Services and Markets Act 2000, any statutes, statutory instruments, regulations, rules, guidance or codes of practice (and modifications and/or reenactments of the same) issued by the Financial Services Authority and/or issued pursuant to any EU Directives on Money Laundering

(including but not limited to the Proceeds of Crime Act 2002 and the Money Laundering Regulations 2003 SI 2003/3075, and the Joint Money Laundering Steering Group guidance).

- The End User agrees to indemnify and keep indemnified Royal Mail against all losses, costs, claims and damages suffered or incurred by Royal Mail directly or indirectly as a result of a breach of any provision of these Minimum Terms by the End User.
- The End User must not withhold any product or service from an Applicant solely on the basis of a Match and the associated Outputs.
- The End User must pay the Licensee all relevant fees as specified by the Licensee for its use of the Product.
- The End User shall:
    - comply in full at all times with all requirements concerning the security processes notified to it by the Licensee in respect of the Product;
    - ensure that all details of the security processes are only provided to employees on a strictly "need to know" basis and for use only in accordance with the Permitted Purpose;
    - ensure that all details concerning the security processes are treated as confidential at all times.

Liability of Royal Mail

- The End User acknowledges that Royal Mail:
    - does not warrant the accuracy and/or completeness of the NCOA® Alert Data;
    - will not be liable for any loss or damage (whether direct or indirect or consequential) however arising from the use by the End User of, or performance of, the NCOA ® Alert Data or the Product, with the exception of death or personal injury caused by Royal Mail's negligence;
    - will not be liable to the End User in respect of any services provided by the Licensee; and
    - will not be obliged in any circumstances to provide NCOA® Alert Data or related services directly to the End User.

Intellectual Property

- The Intellectual Property Rights in NCOA® Alert Data supplied to the End User as part its use of the Product shall remain at all times the property of Royal Mail.

- The End User will not do or permit the doing of anything within its control which will prejudice in any way whatsoever the name of Royal Mail or the rights of Royal Mail in the NCOA® Alert Data and will give immediate notice to Royal Mail upon the End User becoming aware of anything which may prejudice the name of Royal Mail or the rights of Royal Mail in the NCOA® Alert Data.
- The End User undertakes to Royal Mail that it will give immediate notice to Royal Mail upon its becoming aware of any unauthorised use of the NCOA® Alert Data or any other of the Intellectual Property Rights of Royal Mail.

Confidentiality

- The End User shall keep all Outputs confidential and shall not disclose any part of it to any person except as permitted by the Licensee.

Data protection

- The End User shall comply with the requirements of the Data Protection Act 1998 and related statutory instruments, regulations or codes or practice ("DPA") as they apply to the End User's use of the NCOA® Alert Data received through its use of the Product, and makes any notification required under the DPA.
- The End User undertakes that it will not do anything or omit to do anything which would place the Licensee or Royal Mail in breach of the DPA.

Termination

- The Licensee may terminate the End User Agreement at any time if the End User fails to comply with any of the Minimum Terms.
- The End User Agreement shall terminate in respect of the NCOA® Alert Data with immediate effect in the event that the Licensee's agreement with Royal Mail is terminated.
- The End User acknowledges that the Licensee may cease to supply or modify the Product where Royal Mail is required to cease or change the supply of NCOA® Alert Data by law or by a relevant regulatory body.

General

- The End User acknowledges and agrees that these Minimum Terms are given for the benefit of Royal Mail and that Royal Mail may enforce the benefits conferred on it under these Minimum Terms as if it were a party to the End User Agreement, in accordance with the

Contracts (Rights of Third Parties) Act 1999. The End User further acknowledges and agrees that Royal Mail shall bring any action for any unauthorised use of its Intellectual Property Rights in the NCOA® Alert Data on its own behalf.

- Except as set out above, a person who is not a party to the End User Agreement may not enforce any of its provisions under the Contracts (Rights of Third Parties) Act 1999.
- These Minimum Terms may not be varied by the Licensee or the End User without the prior written consent of Royal Mail.
- These Minimum Terms are governed by English law.

EXPERIAN DATA QUALITY – PHONE AND EMAIL VALIDATION

EXPERIAN DATA QUALITY ADDENDUM

In the event of any conflict between the terms of this addendum and the Terms and Conditions, the terms of this addendum shall take precedence to the extent of such conflict.

DEFINITIONS

The following definitions shall apply to the Agreement and where applicable shall supersede any definition in the Terms and Conditions:

1. **Agreed Units;** an agreed number of consumable units (such as professional services days/sessions and/or transactional clicks).
2. **Data Set;** Any data set forming part of the Licensed Materials.
3. **End Of Service Life Policy;** The End Of Service Life Policy available on https://www.edq.com/uk/standard-terms-and-conditions-and-policies/end-of-service-life-policy/
4. **Experian Data Updates**; means any update to Experian data supplied to Client under this Agreement included within the fee for services.
5. **Initial Term/ Term**; As described in the DRS Call-off Schedule 6 Order Form or if not mentioned
6. **Last Ship Date;** the point at which Experian ceases to physically or electronically ship the specific version of the licensed/Experian Materials
7. **Minimum Notice Period;** 90 days to expire on the last day of the Initial Term or any subsequent anniversary of that date or if otherwise stated in CCS Core Terms
8. **New Releases;** means any maintenance release relating to the Experian Materials including, but not limited to, error fixes, minor upgrades and patches (but not including new versions) included within the fee for the Experian Materials;
9. **New Version;** a new version of the Experian Materials not included within the fee for the Experian Materials.
10. **Per Terminal User Data Set**; Experian data specified as such in the 'per terminal user data sets' fact sheet located on https://media.edq.com/4ac170/globalassets/legal/data-sets-and-third-party-software/per-terminal-user-data-sets.pdf or such other URL as Experian notify Clients from time to time.

11. **Third-Party Data Licensor;** any Third-Party providing Third-Party data sets.
12. **Third-Party Data Set;** any Third-Party data forming part of the Experian data.
13. **Third-Party Data Licensor Terms;** any licence terms of a Third-Party Data Licensor relating to a Third-Party data set.
14. **Third-Party Software;** any Third-Party Software forming part of the Experian Materials.
15. **Third-Party Software Provider;** any Third-Party providing Third-Party Software.
16. **Third-Party Software Terms;** any licence terms of a Third-Party Software Provider relating to Third-Party Software.
17. **User**;
    a. an individual authorised to use the Experian Materials and/or services; or
    b. where Client uses the Experian Materials and/or services by means of fully automated use of those Experian Materials and/or services, the device used for that purpose is a user; or
    c. where Client uses a per terminal user data set, an individual workstation or terminal or handheld or other portable device authorised to access the Experian Materials is a user;
    d. where a Client uses software belonging to the Experian Materials an individual workstation or terminal or handheld or other portable device authorized to access the Experian Materials is a user.

1. FEES

1.1. If any Third-Party Data Licensor or Third-Party Software Provider imposes any increase in royalties, Experian shall be entitled to increase fees by the amount of any and all such increase(s) in royalties, subject to Experian notifying the Client of such increase (notice by email shall suffice) at least 120 days before the expiry of the Initial Term or any subsequent anniversary of the commencement date. The increased fees shall apply in place of that originally set out in the schedule unless this Agreement has been terminated prior to the anniversary of the commencement date.

1.2. If any of the services are licensed on a user, copy, application or transaction basis, and a number of users, copies, applications or transactions stated in the schedule is exceeded, the Client shall notify Experian and shall become liable to pay increased licence fees on the basis of the increased number of users, copies, applications or transactions from the date when such permitted use is exceeded.

1.3. The initial contract value and the fees shall be contingent upon the renewal of all of the services purchased or renewed in the previous 12 months (under this Agreement or otherwise), save for any services made available for a development period or related to Agreed Units.

1.4. The Client 30-days prior the expiry of the Initial Term or any subsequent anniversary of the commencement date shall provide Experian with a written declaration in the format provided

by Experian confirming the number of users and any variation to it. Experian reserves the right to audit the Client and to seek confirmation that the number of users declared is accurate.

1.5. All fees are payable annually in advance unless otherwise stated in the Schedule.

2. LICENCE TERMS

2.1. The Experian Materials set out in the schedule are licensed on a "single legal entity" basis. Only the Client's licensed employees, individual contractors or permitted users shall have access to, and use, the Experian Materials for the direct benefit of that single legal entity. Should any other third party, Client group company or other legal entity require access to the Experian Materials the Client will contact Experian promptly and be responsible for payment of any additional fees, including Third-Party data royalties (from the date of use by that Third-Party). Notwithstanding any other term in the Agreement, the liability for such additional fees shall be unlimited. In the event the schedule includes any permitted users, the following additional terms shall apply:

2.2. Permitted users shall have access to the relevant services on the Client's behalf and for the Client benefit only and for no other purpose; and any employees, temporary employees or individual contractors of the permitted user (or terminals where applicable) making use of the services shall count as the Client's users for licensing purposes.

2.3. If the Schedule identifies that any of the services are to be made available for a development period, the Client shall not use (or allow use of) those services for any commercial purposes during that period, and shall not allow use of those services by more than the permitted number of users during that period.

2.4. With respect to any Experian Data Quality Software as a Service (SaaS) services which may be provided under this Agreement, for the duration thereof the Client undertakes to comply with the Fair Use Policy, which is made available to the Client on Experian's website at the following address: https://docs.experianaperture.io/saas-fair-usage-policy.

3. AGREED UNITS

3.1. The Client is required to provide 90-days prior written notice, to expire on the last day of the Initial Term or any anniversary of that date, in the event that the Client wish to reduce the quantity of Experian Materials as stipulated in the schedule, including but not limited to a reduction in the number of users.

3.2. Without prejudice to clause 2.2 above, if this Agreement relates to Agreed Units being made available to the Client, the Client's entitlement to use these Agreed Units shall (unless otherwise stated in the schedule) expire on the last day of the Initial Term irrespective of whether all of the Agreed Units have been used by the Client and without any obligation on Experian's part to provide any refund for unused Agreed Units.

3.3. If this Agreement relates wholly to Agreed Units being made available to Client then notwithstanding the Initial Term referenced in the schedule, this Agreement shall end upon the first to occur of:

3.3.1. all of the Agreed Units having been used; and
3.3.2. the last day of the Initial Term.

4. TECHNICAL SUPPORT

4.1. Experian will provide technical support services in relation to any of the services in accordance with Experian licensed software and supported service and support appendix. Without limitation to the generality of the foregoing, the level of service for Experian Data Quality Software as a Service (SaaS) services shall be outlined under the Service Level Agreement Document, which is made available to the Client on Experian's website at the following address: https://docs.experianaperture.io/saas-services-sla.

4.2. Experian will provide the Client with Experian Data Updates and new releases (which do not include upgrades that Experian identifies as new versions in accordance with Experian's policy in relation to the same from time to time and the End of Service Life Policy. The Client shall install all such Experian Data Updates and new releases as soon as reasonably practicable in order to not affect Experian's ability to offer technical support services.

4.3. New versions will be made available by Agreement and unless otherwise agreed will be subject to an additional charge.

4.4. New versions, new releases and Experian Data Updates made available to the Client shall (unless otherwise agreed) be subject to the provisions of this Agreement as if they formed part of the original Services.

5. ADDITIONAL LICENCES

5.1. If at any time the parties agree to vary the basis on which the Client is using any of the Services by:

5.1.1. varying the number of permitted users;
5.1.2. increasing the number of permitted transactions;
5.1.3. upgrading the Experian Materials;
5.1.4. including additional data sets; and/or
5.1.5. changing the location, application, equipment or operating environment which applies to the services in question.

Any such amendments should be recorded in a variation to the Agreement which shall be amended to incorporate the provisions of such amendments or changes as listed above

6. THIRD-PARTY

6.1. In addition to the rights under clause 10 of the Terms and Conditions, Experian may terminate this Agreement (or any part thereof) immediately by providing notice:

6.1.1. if any claims are made, or in Experian's reasonable opinion are likely to be made, by any Third-Party alleging that its Intellectual Property Rights are infringed by the Client's use of the Experian Materials as permitted by the terms of this Agreement.

6.1.2. if Experian loses the right to distribute any Third-Party data set or Third-Party Software as contemplated by this Agreement, or (subject to Experian giving the Client not less than 12 months' prior written notice) if Experian decides to discontinue the provision of any Experian Materials containing the relevant Third-Party data set or Third-Party Software.

6.2. The Client shall comply with any relevant Third-Party Data Licensor Terms or Third-Party Software Terms imposed on Experian by a Third-Party Data Licensor or Third-Party Software Provider as notified to the Client by Experian or as made available on the Experian website at https://www.edq.com/uk/standard-terms-and-conditions-and-policies/ (or such other URL as Experian informs Clients of from time to time). Notwithstanding any other term in the Agreement, the Client's liability in relation to a breach of this clause shall be unlimited.

6.3. If at any time during the term of this Agreement, any such Third-Party Data Licensor Terms or Third-Party Software Terms change, Experian will notify the Client, and the Client shall be entitled to terminate the use of any Experian Materials materially and adversely affected by the change by notice in writing to Experian.

6.4. In the event of termination in accordance with clause 6.1 or 6.3 above, Experian shall refund the Client on a pro rata basis the amount of any fee paid in advance which relates to use of the relevant Experian Materials during any period following termination. If the schedule indicates that the Client is not being charged royalties in respect of any Experian Materials as a result of the Client having a direct contractual relationship with a Third-Party Data Licensor and/or Third-Party Software Provider, the Client shall indemnify Experian against any claim for unpaid royalties made against Experian by such Third-Party Data Licensor and/or Third-Party Software Provider as result of the use by the Client of the Experian Materials. Notwithstanding any other term in the Agreement, the indemnity provided under this clause shall be unlimited.

6.5. Subject to any contrary provision in any Third-Party licensor Terms or Third-Party Software Terms and other than as specified in the Terms and Conditions, a person who is not a party to this Agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 or otherwise to enforce any term of this Agreement.

EXPERIAN TERMS AND CONDITIONS VERSION 5.0 ("TERMS AND CONDITIONS") ADOPTED: 07/2023

(applicable to all services)

SECTION A: CORE TERMS

These Terms and Conditions shall always apply for the provisions that CCS Core Terms are not covering. CCS Core terms will prevail where there is any conflict with the Experian Terms and Conditions 5.0.

For the avoidance of doubt clause 18 shall always prevail.

1. **PRIMARY OBLIGATIONS AND WARRANTIES**

1.1 Experian shall:

1.1.1 provide the Services in the Territory in accordance with the Specification;

1.1.2 use all reasonable care and skill in the performance of the Services (including in the collection and collation of any data on which the Services are based or which is comprised within the Services); and

1.1.3 use suitably qualified personnel in the provision of the Services.

1.2 The Client shall provide Experian with any information or assistance which the parties have agreed the Client shall provide in order for Experian to perform its obligations under this Agreement and shall use all reasonable endeavours to ensure that any such information provided to Experian is complete, accurate and in the agreed format.

1.3 Each of the parties shall:

1.3.1 where there is a Project Timetable, use all reasonable endeavours to perform its obligations under this Agreement in accordance with the Project Timetable; and

1.3.2 ensure that its personnel, whilst on the premises of the other party, comply with that party's reasonable requirements governing security and health and safety as have been notified to it.

1.4 Each party warrants that:

1.4.1 it has the full power and authority to enter into this Agreement;

1.4.2 it has obtained and will continue to hold all necessary licences, consents, permits and agreements required for it to comply with its obligations under

this Agreement and for the grant of rights to the other party under this Agreement; and

1.4.3 the use by the other party as permitted by this Agreement of any information, data, software, documentation, scorecards and/or services which it provides to the other party shall not infringe any third party Intellectual Property Rights in the Territory.

1.5 The warranties expressly set out in this Agreement are the only warranties that each party gives to the other in respect of the subject matter of this Agreement. All other warranties, representations or terms of equivalent effect that might be implied by law are excluded to the extent permitted by law.

2 TERM

2.1 This Agreement shall be deemed to have commenced on the Commencement Date and, subject to the provisions for early termination set out in this Agreement, shall continue for the Initial Term and thereafter unless terminated by either party serving on the other not less than the Minimum Notice Period to expire on or after the end of the Initial Term.

3 **PAYMENTS AND INVOICING**

3.1 The Client shall pay the fees set out in the Schedule.

3.2 Apart from any sums which are stated in the Schedule to be payable in accordance with a specified payment timetable, all sums payable by the Client to Experian will be invoiced monthly in arrears. All invoices are payable in cleared funds within 30 days after the date of the relevant invoice. If the Client (acting reasonably and in good faith) believes that the amount of any invoice submitted by Experian under this Agreement is incorrect, the Client shall notify Experian of this and the reasons for this belief and of the amount of the invoice which it believes to be incorrect (the "Disputed Amount"). Provided that any such notification and payment of the invoice other than the Disputed Amount have been received by Experian by the due date for payment of the invoice (the "Due Date"), the Client shall be entitled to withhold payment of the Disputed Amount until the date on which the relevant dispute is resolved by the parties. Both parties shall act reasonably and promptly in attempting to resolve any such dispute.

3.3 If any sum payable by the Client to Experian other than a Disputed Amount is not paid in cleared funds by its due date, subject to Clause 3.2, Experian shall be entitled to charge interest on the overdue amount at 2% per annum above Barclays Bank plc's base rate from time to time. Interest will accrue on a daily basis from the due date up to the date of actual payment, after as well as before judgment. In addition, Experian shall, on giving written notice to the Client, be entitled to suspend provision of the Services with immediate effect until the overdue amount is paid in full.

3.4 If under this Agreement the Client agrees in the Schedule to pay a minimum fee over any particular period, and it does not meet such minimum fee requirement in that period, Experian shall be entitled to invoice the Client for the difference between the relevant fees

actually payable in respect of that period and such minimum fee. Any such amount shall be payable to Experian as a debt.

3.5 All sums referred to in this Agreement are exclusive of VAT or any other similar sales or turnover tax (if applicable); such taxes shall be payable on the same payment terms as apply to the sums to which the taxes relate.

3.6 The fees set out in the Schedule will be fixed, save that Experian shall be entitled to increase the fees on the date(s) set out in the Schedule (or, if none, then each anniversary of the Commencement Date) by such percentage as is equal to the percentage increase in the Relevant Index for the most recent period of 12 consecutive months for which figures are available.

4 **NATURE AND USE OF THE SERVICES**

4.1 Experian's services are not intended to be used as the sole basis for any business decision, nor to relieve the Client of its obligation to comply with its own obligations under Applicable Law. Experian Data is based upon data which is provided by third parties, the accuracy and/or completeness of which it would not be possible and/or economically viable for Experian to guarantee. Experian's services also involve models and techniques based on statistical analysis, probability and predictive behaviour. The Client acknowledges that it is prudent to use, and it is responsible for using, the Services as one of a number of factors in its decision-making process, and for determining those other factors. Therefore, Experian will be liable if it fails to comply with its obligation under Clause 1.1.2 but Experian is not able to accept any other liability for:

4.1.1 any inaccuracy, incompleteness or other error in the Experian Data which arises as a result of data provided to Experian by the Client or any third party; or

4.1.2 any failure of the Services to achieve any particular result for the Client or any Permitted User.

4.2 The Client agrees that it will:

4.2.1 use the Services, and/or Experian Materials provided under this Agreement, for the Permitted Purpose only and in accordance with any Documentation

4.2.2 not sell, transfer, sub-license, distribute, commercially exploit or otherwise make available to, or use for the benefit of, any third party any of the Services, and/or Experian Materials provided under this Agreement, except as specifically permitted by this Agreement;

4.2.3 not (and will not allow any third party to) adapt, alter, modify, reverse engineer, de-compile or otherwise interfere with any Experian Materials provided under this Agreement without the prior written consent of Experian or as otherwise permitted by law; and

4.2.4 only take such copies of the Experian Materials as are reasonably required for the use of the Experian Materials in accordance with this Agreement.

5 COMPLIANCE AND AUDIT

5.1 Each party shall in connection with the provision or use of the Services (as appropriate) comply with all Applicable Laws which are applicable to that party.

5.2 Each party shall permit the other (on reasonable notice and during normal working hours and (save where the party being audited is, or is reasonably suspected of being, in material breach of this Agreement) no more than once per Contract Year) to audit the first party's compliance with its obligations under this Agreement in relation to the use of any software, data or other materials. If either party wishes to carry out an additional audit in any Contract Year, it shall reimburse the party being audited for any costs reasonably and properly incurred in connection with supporting such additional audit. The party carrying out the audit shall:

5.2.1 observe the other party's procedures relating to the protection of confidential information about any clients or customers of the other party; and

5.2.2 take all reasonable steps to minimise disruption to the other party's business during such audit.

5.3 User Access Devices are (where applicable) provided by Experian to enable the Client to access and use the Services in accordance with the terms of this Agreement. The Client shall ensure that any User Access Device(s) are not copied, interfered with and/or used in any unauthorised way.

5.4 It is the Client's responsibility to inform Experian of any unauthorised use and/or disclosure of any User Access Device so that Experian can suspend or disable that User Access Device as appropriate. The Client shall remain liable for any and all fees for the Services incurred in connection with the use of any User Access Device, until the Client has informed Experian.

5.5 Each party will cooperate and share information with the other as reasonably necessary from time to time (including in circumstances where the parties may individually or collectively have caused harm to end consumers) to ensure that both parties discharge their regulatory obligations, and in order to help achieve positive consumer outcomes.

5.6 Consumer Duty (where applicable). Without prejudice to the general obligations under Clause 5.5 in respect of consumer harm, each of the parties agree that in the event Consumer Duty applies in the provision or use of the Services (as appropriate), the parties shall comply with Consumer Duty and the following provisions will apply:

5.6.1 Where Consumer Duty applies in the Client's use of Services the Client must determine itself how to distribute products in a way that supports good customer outcomes.

5.6.2 Permitted Purpose. The Client must comply with the provisions of Clause 15.1 including (but not limited to) using the Services in accordance with the

Permitted Purpose and any other provisions relating to use of the Services or restrictions on the use of the Services set out in the Schedule. In addition to any audit rights described within this Clause 5, Experian reserves the right to assess and monitor whether the Client is in compliance with the Permitted Purpose and any usage rights and restrictions in the Schedule and its obligations under this Agreement. The Client will provide Experian with any materials Experian reasonably requests in order to conduct such an assessment. The Client is also obligated to report back to Experian any non-compliances with the Permitted Purpose and any usage rights or restrictions. In the event that in Experian's reasonable judgement the Client's use of the Services is not compliant with the Permitted Purpose or any usage rights and restrictions set out in the Schedule or the Client is in breach of its obligations in relation to Consumer Duty, the following process applies:

5.6.2.1 Experian will notify the Client in writing specifying the non-compliance and grant the Client 15 days to remedy any non-compliances and ensure its use of the Services complies with the Permitted Purpose and any usage rights and restrictions.

5.6.2.2 If Experian in its sole discretion judges the Client to still be non-compliant after such remediation period set out in Clause 5.6.2.1, Experian reserves the right to suspend the Client's use of the Services by serving written notice and grant the Client a period of remediation of 28 days after receipt of the suspension notice within which to remedy the non-compliance.

5.6.2.3 In the event of the non-compliance being remedied within the remediation period set out in Clause 5.6.2.2 Experian will lift the suspension. Otherwise, Experian reserves the right to terminate this Agreement immediately by serving written notice to the Client in the event that either:

5.6.2.3.1 the non-compliance is not capable of remedy; or

5.6.2.3.2 the non-compliance is capable of remedy and the Client has failed to remedy the non-compliance in accordance with the timelines set out in Clause 5.6.2.2 above.

5.6.3 Cross-cutting Rules. The following provisions apply:

5.6.3.1 the parties agree to act in good faith towards retail customers;

5.6.3.2 the parties must avoid causing foreseeable harm to retail customers; and

5.6.3.3 the parties must enable and support retail customers to pursue their financial objectives.

5.6.4 Pricing. The Client acknowledges that it is its responsibility to ensure it provides fair value and complies with pricing obligations it has under Consumer Duty and the Client confirms it will evidence its compliance with PRIN 2A.4 under Consumer Duty.

5.6.5 Monitoring. Experian reserves the right to assess and monitor whether the Client is in compliance with Consumer Duty and is providing good outcomes for retail customers. The Client must monitor the outcomes retail customers receive from any Experian products, the communications it has with retail customers and the customer support it provides to retail customers. The Client agrees to share with Experian any documentation or management information ("MI") the Client generates as a result of its outcome monitoring involving Experian products.

5.6.6 Reporting. The following provisions apply:

5.6.6.1 if the Client identifies that it or another firm in its distribution chain is not delivering good outcomes for retail customers, it must promptly notify Experian; or

5.6.6.2 where either party identifies or becomes aware of a communication produced by another firm in its distribution chain that is not delivering good outcomes for retail customers, it must promptly notify the issue to the relevant firm in the distribution chain (which may include the other party to this Agreement); and

5.6.6.3 notwithstanding any suspension of the Services, each party is obligated under Consumer Duty to notify the Financial Conduct Authority if it becomes aware that any other firm in the distribution chain is not or may not be complying with Principle 12 under Consumer Duty. Each party shall be responsible for its own costs incurred in such reporting.

5.7 Without prejudice to the general obligations under Clause 5.1,each of the parties shall in connection with this Agreement:

5.7.1 comply with the Anti-Corruption Requirements and the Anti-Slavery Requirements;

5.7.2 not engage in any activity, practice or conduct which would constitute either a UK tax evasion facilitation offence under section 45(1) of the Criminal Finances Act 2017, a foreign tax evasion facilitation offence under section 46(1) of the Criminal Finances Act 2017.

5.8 Each party shall have and shall maintain in place throughout the Term its own policies and procedures to ensure compliance with Clause 5.6, including adequate procedures under the Bribery Act 2010, and will enforce them where appropriate.

5.9 Each party shall promptly report to the other:

5.9.1 any request or demand for any undue financial or other advantage of any kind received in connection with this Agreement;

5.9.2 any slavery or human trafficking in a supply chain which has a connection with this Agreement;

5.9.3 any request or demand from a third party to facilitate the evasion of tax within the meaning of Part 3 of the Criminal Finances Act 2017, in connection with the performance of this Agreement.

5.10 If, as a result of (a) any changes in Applicable Law (including any reasonable interpretation thereof); (b) any changes in the supply of third party data used in connection with the Services; or (c) a security vulnerability (other than a Personal Data Breach) which Experian reasonably considers may cause consumer harm, Experian considers the Services to have become Affected Services Experian will be entitled to do one of the following (as applicable) on giving prior written notice to the Client (and Experian shall, where possible, use reasonable endeavours to give three months written notice):

5.10.1 suspend and modify the Affected Services as necessary; or

5.10.2 procure alternative data, the same as or similar to the data used in the Affected Services; or

5.10.3 terminate this Agreement without liability in respect of those Affected Services.

6 **CONFIDENTIALITY**

6.1 Each party shall, in respect of the Confidential Information for which it is the recipient:

6.1.1 keep the Confidential Information strictly confidential and not use or disclose any part of such Confidential Information to any person except as permitted by or as required for the performance of the recipient's obligations under this Agreement; and

6.1.2 take all reasonable steps to prevent unauthorised access to the Confidential Information.

6.2 The parties may disclose the Confidential Information for which it is the recipient to, and allow its use in accordance with this Agreement by, the following (as long as the conditions in Clause 6.3 are met):

6.2.1 employees and officers of the recipient who necessarily require it as a consequence of the performance of the recipient's obligations under this Agreement;

6.2.2 the recipient's auditors and professional advisors solely for the purposes of providing professional advice and any other persons or bodies having a legal right or duty to have access to, or knowledge of, the Confidential Information in connection with the business of the recipient;

6.2.3 the recipient's Group Companies for reasonable reporting purposes;

6.2.4 (in the case of the Client being the recipient) Permitted Users to the extent required to exercise the Permitted User Rights;

6.2.5 (in the case of Experian being the recipient), agents and/or sub-contractors of Experian who reasonably require it as a consequence of the performance of Experian's obligations under this Agreement.

6.3 As a condition of the rights set out in Clause 6.2 the party wishing to exercise the rights must:

6.3.1 ensure that any person to whom it discloses Confidential Information is under an obligation of confidentiality which is substantially the same as set out in this Clause 6 in relation to such Confidential Information; and

6.3.2 procure that such persons observe the restrictions in this Clause 6.

6.4 The restrictions in Clause 6.1 do not apply to any information to the extent that it:

6.4.1 is or comes within the public domain other than through a breach of Clause 6.1; or

6.4.2 is in the recipient's possession (with full right to disclose) before receipt from the other party; or

6.4.3 is lawfully received from a third party (with full right to disclose); or

6.4.4 is independently developed by the recipient without access to or use of the Confidential Information of the disclosing party; or

6.4.5 is required to be disclosed by law or by a court of competent jurisdiction or by any regulatory body or in accordance with the rules of any recognised stock exchange.

6.5 The parties acknowledge that from time to time the parties may discuss the provision of additional and/or new products and services by Experian to the Client and/or that Experian may bid to provide new products and/or services to the Client (whether as part of a formal tender process or not). In such circumstances the parties agree that:

6.5.1 the terms of this Clause 6 shall apply to any such discussions or bid (including any documents issued in relation to the bid) and any ideas and output developed as part of those discussions and/or bid;

6.5.2 references in this Clause 6 to a recipient's obligations and the purposes of this Agreement shall be deemed to refer to the assessment of the provision of goods/services by Experian to the Client; and

6.5.3 the recipient shall return to the other party all materials containing the other party's Confidential Information immediately upon demand by the other party.

6.6 Where Experian processes Personal Data contained within Client Data, the terms of Clause 18 shall govern such processing and Personal Data contained within Client Data shall not therefore be considered Confidential Information for the purposes of this Clause 6.

7 **INTELLECTUAL PROPERTY RIGHTS**

7.1 All Intellectual Property Rights in the Client Materials will remain vested in the Client (or its relevant licensors) and to the extent that any rights in such materials vest in Experian by operation of law, Experian hereby assigns such rights to the Client.

7.2 All Intellectual Property Rights in the Experian Materials and the Derivative Output will remain vested in Experian (or its relevant licensors) and to the extent that any rights in such data or materials vest in the Client by operation of law, the Client hereby assigns such rights to Experian.

7.3 Each party:

7.3.1 acknowledges and agrees that it shall not acquire or claim any title to any of the other party's Intellectual Property Rights (or those of the other party's licensors) by virtue of the rights granted to it under this Agreement or through its use of such Intellectual Property Rights;

7.3.2 agrees that it will not, at any time, do, or omit to do, anything which is likely to prejudice the other party's ownership (or the other party's licensors' ownership) of such Intellectual Property Rights; and

7.3.3 agrees not to remove, suppress or modify in any way any proprietary marking, including any trade mark or copyright notice, on or in the materials of the other party and agrees to incorporate any such proprietary markings in any copies it takes of such materials.

8 THIRD PARTY CLAIMS

8.1 Subject to Clause 8.2, each party shall fully indemnify the other party against:

8.1.1 any amounts paid by the indemnified party to any third party as a result of or in connection with any claim which that third party brings against the indemnified party alleging that its Intellectual Property Rights are infringed by the provision by the indemnifying party to the indemnified party of the indemnifying party's Materials or the use of the indemnifying party's Materials by the indemnified party as permitted by the terms of this Agreement; and

8.1.2 any associated legal expenses reasonably and properly incurred.

8.2 The indemnities in Clause 8.1 shall not apply to the extent that any claim arises as a result of use of any infringing Materials supplied or developed by the indemnified party, and are subject to the indemnified party:

8.2.1 notifying the indemnifying party promptly on becoming aware of any matter or claim to which the indemnity might relate;

8.2.2 not making any admission, settlement or payment in respect of such matter or claim, other than a payment made pursuant to a court order, without the prior written consent of the indemnifying party (such consent not to be unreasonably withheld or delayed); and

8.2.3 allowing the indemnifying party, where appropriate, to appoint legal advisers of its choice and to conduct and/or settle negotiations and/or proceedings relating to such matter or claim and the indemnified party shall comply with the indemnifying party's reasonable requests in the conduct of any such negotiations and/or proceedings.

8.3 If any claims are made, or in Experian's reasonable opinion are likely to be made, by any third party alleging that its Intellectual Property Rights are infringed by the Client's use of the Experian Materials as permitted by the terms of this Agreement, Experian may at its sole option and expense:

8.3.1 procure for the Client the right to continue using the relevant Experian Materials (or any part of them) in accordance with the terms of this Agreement; and/or

8.3.2 modify the relevant Experian Materials to avoid the infringement or replace the relevant Experian Materials with non-infringing materials, whilst still providing the same, or substantially similar, functionality to the infringing materials.

9 LIMITS ON LIABILITY

9.1 Neither party excludes or limits its liability to the other for any of the following (and nothing in this Agreement shall be construed as excluding or limiting such liability):

9.1.1 for breach of its obligations under section 12 Sale of Goods Act 1979 or section 2 Supply of Goods and Services Act 1982;

9.1.2 for personal injury or death resulting from its negligence or that of its employees, agents and/or sub-contractors by operation of Section 2(1) of the Unfair Contract Terms Act 1977;

9.1.3 for breach of Clause 6;

9.1.4 for any matter which it would be illegal for that party to exclude and/or limit, or attempt to exclude and/or limit, its liability; or

9.1.5 for that party's fraud or fraudulent misrepresentation.

9.2 The liability of each party to the other (whether in contract, negligence, breach of statutory duty or under any indemnity or otherwise) in respect of:

claims for the damage to or loss of tangible property (excluding claims for loss or corruption of, or damage to, data contained on any tangible media) shall be limited to £1 million per claim or series of claims arising from any one incident.

9.3 Except as provided in Clauses 9.1, 9.2, and 9.4, the liability of each party to the other in respect of any claims (whether in contract, negligence, for breach of statutory duty or under any indemnity or otherwise) brought under or in connection with this Agreement shall be limited as follows:

9.3.1 for all claims arising in the first Contract Year, liability shall be limited in aggregate to the Initial Contract Value;

9.3.2 for all claims arising in any subsequent Contract Year liability shall be limited in aggregate to the fees (excluding VAT) paid by the Client to Experian under this Agreement in the previous Contract Year.

9.4 The limitations in Clause 9.3 shall:

9.4.1 not apply to the indemnity given under Clause 8.1;

9.4.2 not apply to any liability of either party under Clause 18.5;

9.4.3 be in addition to the obligation of the Client to pay the fees and charges under this Agreement.

9.5 Subject to Clause 9.1, neither party shall be liable to the other (whether in contract, negligence, for breach of statutory duty or under any indemnity or otherwise) for:

9.5.1 any indirect or consequential loss;

9.5.2 the following types of financial loss: loss of profits; loss of earnings; loss of business or goodwill; even if that party had notice of the possibility of the other party incurring such losses; or

9.5.3 the following types of anticipated or incidental losses: loss of anticipated savings; increase in bad debt; failure to reduce bad debt; even if that party had notice of the possibility of the other party incurring such losses.

10 TERMINATION

10.1 Either party shall be entitled to terminate this Agreement immediately by serving written notice on the other party in the following circumstances:

10.1.1 if the other party commits a material breach of any of its obligations under this Agreement which is not capable of remedy;

10.1.2 if the other party commits a material breach of any of its obligations under this Agreement which is not remedied within 28 days after receipt of a notice from the party not in breach specifying the breach, requiring its remedy and making clear that failure to remedy may result in termination;

10.1.3 if the other party has passed a resolution for its winding up or is subject to a petition presented to any court for its winding-up (save, in either case, for a voluntary winding-up for the purpose of a voluntary reconstruction or amalgamation), is the subject of an application for administration, or a notice

of intention to appoint an administrator, filed at any court, or is dissolved or declared bankrupt, or has a receiver, administrator or administrative receiver appointed over all or part of its assets, or enters into an arrangement with its creditors, or suspends or threatens to suspend payment of its debts or is unable to pay its debts within the meaning of section 123 Insolvency Act 1986, or ceases to trade or takes or suffers any similar action;

10.1.4 upon becoming aware at any time that Sanctions apply to or otherwise target the other party or the other party is on an applicable Sanctions list maintained by such Sanctions Authority as apply to the party giving notice ("Notifying Party"), and that such listing prevents or materially affects the Notifying Party's ability to (as applicable) provide or receive the Services or give or receive payment or makes it impossible, impracticable or unlawful for the Notifying Party to perform any of its obligations or exercise any of its rights under this Agreement. In addition, if Experian becomes aware that Sanctions apply to or otherwise target a Permitted User of the Client or a Permitted User is on a Sanctions list, Experian shall be entitled to terminate the Permitted User Rights immediately on serving written notice on the Client. In the event that Experian becomes aware that Sanctions apply to or otherwise target a Group Company of the Client or the Group Company of a Client is on a Sanctions list or the Client is directly or indirectly owned or controlled by a Sanctions Restricted Person, Experian shall be entitled to either suspend the Services provided under this Agreement or terminate this Agreement, even if Sanctions do not apply to or otherwise target the Client itself or the Client itself is not on a Sanctions list;

10.1.5 where a Change in Applicable Law renders some or all of the activities of that party in connection with this Agreement illegal or unlawful and no action that party could reasonably be expected to take can make such activities legal and lawful.

10.2 Termination of this Agreement (or of any element of it) shall not affect any rights, obligations or liabilities of either party:

10.2.1 which have accrued before termination; or

10.2.2 which are intended to continue to have effect beyond termination.

10.3 Upon termination of this Agreement (or the relevant elements of it) and subject to Clause 10.4:

10.3.1 the parties shall each promptly return the Confidential Information of the other party to its owner;

10.3.2 the Client shall, at Experian's request either return any Experian Materials to Experian or destroy such materials and, if destroyed, provide a certificate stating that such materials have been destroyed; and

10.3.3 Experian shall promptly return any Client Materials to the Client on request.

10.4 The obligations under Clause 10.3 shall not apply where it is necessary to retain any Confidential Information, Experian Materials or Client Materials to exercise any rights granted under this Agreement which are intended to survive termination of this Agreement and/or to the extent that retention is required by law or any applicable governmental or regulatory authority, for audit requirements or handling of any consumer complaints, or where electronic records have been automatically backed up to a backup or recovery system in the ordinary course of business for disaster recovery purposes. The terms of this Agreement (including Clause 6 and 18) shall continue to apply to any information or materials retained.

10.5 The licences granted by Experian under this Agreement will automatically expire on termination of this Agreement for any reason and the Client shall, other than as set out in Clause 10.4, cease to use all Experian Materials (unless any licence is expressed in the Schedule to be perpetual in which case such licence and any terms relating to the extent and/or exercise of that licence shall remain in force notwithstanding termination of this Agreement, except if termination is by Experian pursuant to Clause 10.1).

11 FORCE MAJEURE

11.1 Neither party will be liable for any delay or failure in the performance of its obligations under this Agreement if such delay or failure is due to an event of Force Majeure.

11.2 If the Force Majeure persists for a period of 28 days or more, the party not claiming Force Majeure may give notice to the other to terminate this Agreement with effect from a date specified in the notice without penalty or other liability (except for any liability on the Client to pay accrued fees).

12 SEVERANCE

12.1 If any court or competent authority finds that any provision of this Agreement (or part of any provision) is invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed to be deleted, and the validity and enforceability of the other provisions of this Agreement shall not be affected.

12.2 If any invalid, unenforceable or illegal provision of this Agreement would be valid, enforceable and legal if some part of it were deleted, the parties shall negotiate in good faith to amend such provision such that, as amended, it is legal, valid and enforceable, and, to the greatest extent possible, achieves the parties' original commercial intention.

13 NOTICES

13.1 Any notices to be sent by one party to the other in connection with this Agreement except for the service of Court proceedings shall be in writing and shall be sent by first class post (or equivalent service offered by the postal service from time to time) to either the addresses of each party as set out in this Agreement or to the registered office addresses of each party (and in the case of notices sent to Experian, with a copy to Experian's Legal Department).

13.2 Notices shall be deemed to have been duly given two clear days after the date of posting.

13.3 If either party notifies the other party of a change to its details for the purposes of Clause 13.1, such notification shall only be effective on the date specified in such notice or seven days after notice is given, whichever is later.

14 GENERAL

14.1 If either party fails to exercise a right or remedy that it has or which arises in relation to this Agreement, such failure shall not prevent that party from exercising that right or remedy subsequently in respect of that or any other incident.

14.2 A waiver of any breach or provision of this Agreement shall only be effective if it is made in writing and signed on behalf of the party who is waiving the breach or provision. Any waiver of a breach of any term of this Agreement shall not be deemed a waiver of any subsequent breach and shall not affect the enforceability of any other term of this Agreement.

14.3 This Agreement and all matters arising out of it shall be governed by, and construed in accordance with, the laws of England. The English courts shall have exclusive jurisdiction over any claim or matter which may arise out of or in connection with this Agreement.

14.4 Variations of this Agreement shall not be effective unless recorded in writing signed by the parties (signature may be made by electronic signature); variations in electronic form shall not count as variations recorded in writing. However, variations to the Schedule made in accordance with any agreed change control procedure shall be effective.

14.5 Neither party may assign, transfer, charge or deal in any other manner with this Agreement or any of its rights under it, or purport to do any of these things, without the prior written consent of the other party (such consent not to be unreasonably withheld or delayed).

14.6 This Agreement sets out all the terms agreed between the parties relating to the subject matter of this Agreement and supersedes any previous agreement between the parties (whether oral or written) relating to the same subject matter. Each party acknowledges that in entering into this Agreement it does not rely on, and shall have no remedies in respect of, any warranty or representation (whether made innocently or negligently) that is not set out in this Agreement. Nothing in this Clause shall limit or exclude any liability for fraudulent misrepresentations.

14.7 Except as expressly provided in Clause 19.1.2, a person who is not a party to this Agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 or otherwise to enforce any term of this Agreement. The rights of the parties to terminate, rescind or agree any variation, waiver or settlement under this Agreement are not subject to the consent of any other person.

14.8 Each party shall, at the reasonable request and cost of the other party, do whatever is reasonably required to give the other party the full benefit of all the provisions of this Agreement.

14.9 This Agreement may be executed in any number of counterparts.

14.10 Nothing in this Agreement is intended to, or shall, operate to:

14.10.1 create a partnership or joint venture of any kind between the Client and Experian;

14.10.2 authorise either party to act as agent for the other party; or

14.10.3 authorise either party to act in the name or on behalf of, or to otherwise bind, the other party in any way.

14.11 In this Agreement:

14.11.1 any reference to a statutory provision includes a reference to any modification or re-enactment of it from time to time;

14.11.2 references to Clauses are to the clauses of the particular section of the Experian Terms and Conditions in which they appear, unless reference is made to another set of Experian Terms and Conditions;

14.11.3 references to schedules are to the Schedule;

14.11.4 the singular includes the plural and vice versa;

14.11.5 the headings are for ease of reference only and shall not affect the construction or interpretation of this Agreement;

14.11.6 where any matter is to be agreed, such agreement must be recorded in writing; and

14.11.7 wherever the words "including", "include", "includes" or "included" are used they shall be deemed to be followed by the words "without limitation" unless the context otherwise requires.

14.12 The contents of the Schedule shall prevail over the contents of these Terms and Conditions to the extent of any conflict or inconsistency.

SECTION B: DATA AND MATERIALS TERMS

These terms relating to data and materials are supplemental to the Core Terms, and apply only if either party provides data and/or materials to the other party.

15 PROVISION OF DATA AND MATERIALS

15.1 Experian grants the Client (subject to Clauses 4.2 and 10.5) a non-exclusive non-transferable licence to use any Experian Materials provided as part of the Services for the Permitted Purpose on any licence terms identified in the Schedule. Such licence to use any Experian Materials is granted to the Client for the benefit of the Client's UK business. The licence granted under this Clause is made separately in respect of each individual element of the Experian Materials and commences on the day that each element of the Experian Materials is first made available to the Client. The Client shall not upload any Experian Materials into

any third party applications including any artificial intelligence ("AI") technologies including, but not limited to, large language models and generative AI and any other artificial intelligence type technologies.

15.2 The use by the Client of any Services which are dependent upon data derived from a Data Sharing Scheme is conditional upon the Client complying with the relevant Data Sharing Scheme Rules which are in force from time to time and any requirements in order to comply with Applicable Law.

15.3 If at any time the condition in Clause 15.2 is not satisfied, Experian shall be entitled to discontinue the provision of any and all Services which utilise data from the relevant Data Sharing Scheme.

16 CLIENT OBLIGATIONS

16.1 In addition to the obligations set out in the Clause 5.3, the Client shall comply with Experian's reasonable instructions and security guidelines relating to access to Experian's systems, including those set out at https://ssp.uk.experian.com/securecontrol/securityGuidelines.html.

16.2 In order to protect the integrity of the Experian Data used in connection with the Services, the Client shall:

16.2.1 comply with Experian's reasonable instructions and guidelines relating to data security, including those set out at https://www.experian.com/content/dam/marketing/na/procurement/TPSMS029-Experian-Security-Requirements.pdf and where included, in the Schedule;

16.2.2 not copy, interfere with and/or use in any unauthorised way any digital certificate, web certificate or any other security device provided by Experian.

17 USE OF CLIENT MATERIALS

17.1 The Client grants Experian (subject to Clause 10.3) a royalty free, non-exclusive, non-transferable licence to use (and copy) the Client Materials solely for the purposes of:

17.1.1 performing this Agreement; and

17.1.2 complying with any requests made to Experian under statute and/or regulation.

18 DATA PROTECTION

18.1 Without prejudice to the general obligations under Clause 5.1 each of the parties shall in the provision or use of the Services (as appropriate) comply with all applicable Data Protection Legislation.

18.2 Each party warrants that it shall implement appropriate technical and organisational measures to ensure a level of data security relating to the Personal Data of the other party appropriate to the risk presented by the Processing.

18.3 The Client instructs Experian to, and agrees that Experian may, process the Client Data for the Agreement Purposes.

18.4 There are circumstances in which Experian will or may be a Processor of Client Data. When, and to the extent that from time to time, Experian is a Processor of Client Data:

18.4.1 Experian shall process the Client Data only in accordance with the Client's documented instructions referred to in Clause 18.3 (including with regard to transfers of Personal Data to a third country) and any other instructions agreed by the parties from time to time, unless Experian is required to process the Client Data to comply with Applicable Law (in which case, Experian shall inform the Client of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest);

18.4.2 Client authorises the international transfer of Client Data where Experian is required to conduct an international transfer in order to comply with UK Law (in which case, Experian shall inform the Client of that legal requirement before processing, unless UK Law prohibits such communication on important grounds of public interest);

18.4.3 Experian shall ensure that persons authorised to process the Client Data have committed themselves to confidentiality;

18.4.4 Client provides general authorisation to Experian's use of Sub-processors to provide Processing activities on Client Data on behalf of the Client. The details of Experian's current Sub-processors are available via the following link: https://www.experian.co.uk/crain/data-sub-processors. In the event that Experian adds or replaces any Sub-processors during the term of this Agreement, Experian will update this website and provide Client with a mechanism to obtain notice of that update. In line with Article 28(2) of UK GDPR the Client has the opportunity to object to such changes. The appointment of any Sub-processor shall not relieve Experian of its obligations under this Agreement.

18.4.5 Experian shall ensure that where Experian appoints another Processor as contemplated by Article 28(4) of the UK GDPR, that Processor is subject to contract obligations as required by that Article;

18.4.6 Experian shall take into account the nature of the Processing Experian carries out as a Processor of Client Data and assist the Client by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Client's obligation to respond to requests for exercising the data subject rights laid down in Chapter III of the UK GDPR;

18.4.7 Experian shall assist the Client in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the UK GDPR, taking into account the nature of the Processing Experian carries out, and the information available to Experian, in its capacity as a Processor of Client Data;

18.4.8 Experian shall (at the request of the Client) comply with its obligations relating to the return or destruction of data under Clause 10.3, and to audit under Clause 5;

18.4.9 Experian shall (at the request of the Client) provide the Client with any information which it is reasonable for Experian to provide to allow the Client to demonstrate compliance with Article 28 of the UK GDPR;

18.4.10 Experian shall comply with its obligations under Article 28(3) of the UK GDPR to inform the Client immediately if in the opinion of Experian any instruction of the Client referred to in Clause 18.4.1 infringes the UK GDPR or any other relevant data protection provision;

18.4.11 Experian shall notify the Client without undue delay after becoming aware of a Personal Data Breach relating to the Client Data.

18.5 Subject to Clause 18.6, if, pursuant to Article 82(4) UK GDPR, one party (the "Paying Party") has been held liable to pay compensation to a data subject for damage caused (in whole or part) by the other party ("Other Party"), the Paying Party shall, as envisaged under Article 82(5) UK GDPR, be entitled to recover from the Other Party (as a debt) any part of such compensation corresponding to damage for which the Other Party was responsible.

18.6 Following receipt of a claim (or notification of an intention to make a claim) from a data subject to which Article 82(4) UK GDPR may apply:

18.6.1 the party in receipt of the claim shall promptly notify the other party of the claim;

18.6.2 neither party shall make any admission of liability, settlement or payment in respect of such claim, other than a payment made pursuant to a court order, without the prior written consent of the other party (such consent not to be unreasonably withheld or delayed); and

18.6.3 each party shall provide such cooperation and assistance as is reasonably required by the other party in connection with the claim.

SECTION C: PERMITTED USERS

These terms relating to Permitted Users are supplemental to the Core Terms and shall apply only where the Schedule states that there are Permitted Users in connection with this Agreement.

19 PERMITTED USERS

19.1 It may be of benefit to the Client for agreed third parties to have certain access to the Services. The Client shall therefore be entitled to allow Permitted Users to exercise the Permitted User Rights. In order to achieve this without the need for each Permitted User to contract directly with Experian, the Client agrees as follows:

19.1.1 the Client shall procure that each Permitted User complies with all relevant provisions of this Agreement, including the obligation that the Permitted Users use the Services for the Permitted Purpose only; and

19.1.2 pursuant to the Contracts (Rights of Third Parties) Act 1999, the terms of this Agreement shall be enforceable by each Permitted User (to the extent permitted by law and subject to the terms of this Agreement including Clause 19.1.3) as if each Permitted User were a party to this Agreement;

19.1.3 the terms of Clause 9 (Limits on Liability) shall apply on an aggregate basis across all claims that may be brought by the Client and/or a Permitted User under or in connection with this Agreement;

19.1.4 unless expressly agreed otherwise in the Schedule, a Permitted User must at all times be a Client Group Company in order to have access to the Services as set out in this Agreement. If any Permitted User is no longer a Client Group Company ("ExPermitted User"), the rights of the relevant Permitted User will automatically terminate (without further notice and without liability to Experian) on the date it ceases to be a Client Group Company and the Client will be liable for any acts or omissions of the Ex-Permitted User as if they were the acts or omissions of the Client;

19.1.5 where an Ex-Permitted User has any Experian Materials, the Client shall inform Experian in writing, and shall ensure that such Ex-Permitted User:

19.1.5.1 stops use of and has no further possession of or access to such Experian Materials; and

19.1.5.2 returns to the Client all copies of Experian Materials and any other equipment or software which is the property of Experian in its possession or control; and

19.1.5.3 deletes any remaining copies of such Experian Materials from its computer system and any other medium on which it is stored.

19.1.6 if the Client's rights under this Agreement terminate (for whatever reason), the Permitted Users Rights shall also automatically terminate (without further notice and without liability to Experian).

19.2 References to Client Materials in this Agreement shall be deemed to include data and materials provided by Permitted Users.

SECTION D: DEFINITIONS

In this Agreement the following words and expressions shall have the following meanings:

Words or Expression	**Meaning**

Affected Services	Services which Experian (in its reasonable opinion) considers that it can no longer provide in accordance with their Specification or that it cannot provide at all as a consequence of the trigger events set out in Clause 5.10;
Agreement Purposes	The purposes of Experian providing the Services as contemplated by this Agreement, and for such other purposes as the parties may agree from time to time;
Anti-Corruption Requirements	All Applicable Law relating to anti-bribery and anti-corruption including the Bribery Act 2010;
Anti-Slavery Requirements	All Applicable Law relating to anti-slavery and human trafficking including the Modern Slavery Act 2015;
Applicable Law	All legislation, regulations, legally binding rules, policies, guidance, codes of practice, instructions, notices, publications or recommendations issued by any governmental, statutory or regulatory body and any legally binding industry codes of conduct or guidelines and any other rules having equivalent force which are applicable to the provision or use of the Services under this Agreement;
Change in Law	the coming into effect of a new Applicable Law or a change in Applicable Law or a fundamental change in the judicial interpretation of Applicable Law after the date of this Agreement;
Client Data	Any of the data (including Personal Data) and/or databases supplied by the Client and provided to Experian in connection with this Agreement but excluding any data supplied to the Client by Experian;
Client Materials	Any of the items provided to Experian by the Client in connection with this Agreement and includes Client Data;
Commencement Date	The Commencement Date set out in the Schedule or in the absence of such date then the date that on which this Agreement is signed by the final signatory;

Confidential Information	Any and all information relating to the trade secrets, operations, processes, plans, intentions, product information, prices, know-how, designs, customer lists, market opportunities, transactions, affairs and/or business of the parties and/or to their customers, suppliers, clients or Group Companies in or on any medium or format;
Word or Expression	**Meaning**
Consumer Duty	As set out in Principle 12 and PRIN 2A of the Principles for Business section of the Financial Conduct Authority ("FCA") Handbook and any related rules or guidance issued by the FCA relating to the delivery of good customer outcomes for retail customers;
Contract Year	A twelve calendar month period from the Commencement Date or any anniversary of the Commencement Date, or, if this Agreement is for a Term of less than twelve calendar months, the Term;
Controller	means the definition specified in the Data Protection Legislation;
Core Terms	The provisions set out in Section A and the definitions set out in Section D of these Terms and Conditions;
Data Protection Legislation	All Applicable Law relating to data protection and privacy;
Data Sharing Scheme	Any scheme, programme, membership, information exchange, or other arrangement where certain data sharing activities are carried out subject to the relevant Data Sharing Scheme Rules;
Data Sharing Scheme Rules	The rules of the relevant Data Sharing Scheme;
Derivative Output	Information, data and materials that are derived, prepared or generated by Experian and/or its sub-contractors pursuant to (and/or as a consequence of) the Services, including search footprints but excluding the Client Materials themselves
Documentation	Any or all of the Specification, user documentation, product documentation, technical documentation including guidelines relating to data security and access and/or statements of functionality;

Experian Data	Any of the data (including Personal Data) and/or databases and/or scores supplied by Experian to the Client in connection with this Agreement but excluding the Client Data;
Experian Materials	Software and any materials, Documentation, Scorecards or other items developed and/or licensed by Experian to the Client in connection with this Agreement and includes Experian Data;
Force Majeure	Any act of government or state, civil commotion, epidemic, fire, flood, industrial action or organised protests by third parties, natural disaster, war, failure of payment systems, or any event beyond the reasonable control of the party claiming to be excused from performance of its obligations;
Group Company	any company which is in relation to Experian or (as the case may be) the Client, a subsidiary, holding company or subsidiary of a holding company as the terms "subsidiary" and "holding company" are defined by section 1159 of the Companies Act 2006. "Experian Group Company" and "Client Group Company" shall be interpreted in this way;
Initial Contract Value	The greater of (1) the amounts (excluding VAT) payable by the Client under this Agreement in the first Contract Year as specified in the Schedule; and (2) the amounts (excluding VAT) actually paid by the Client under this Agreement in the first Contract Year;
Initial Term	The period specified as such in the Schedule;
Intellectual Property Rights	Copyright, database right, domain names, patents, registered and unregistered design rights, registered and unregistered trade marks, and all other industrial, commercial or intellectual property rights existing in any jurisdiction in the world and all the rights to apply for the same;
Word or Expression	**Meaning**
Materials	means Client Materials or Experian Materials, as appropriate;

Minimum Notice Period	The minimum period of notice to be served by either party to terminate this Agreement as set out in the Schedule (and if none is specified 12 months);
Permitted Users	The permitted users identified in the Schedule;
Permitted User Rights	The rights of the Permitted User set out in the Schedule;
Permitted Purpose	Unless otherwise set out in the Schedule, the internal business purposes of the Client and not in any event for the provision of bureau services to any third parties.
Personal Data	The definition specified in the Data Protection Legislation;
Personal Data Breach	The definition specified in the Data Protection Legislation;
Processing	The definition specified in the Data Protection Legislation;
Processor	The definition specified in the Data Protection Legislation;
Project Timetable	Any timetable expressly set out or referred to in the Schedule or otherwise agreed between the parties from time to time;
Relevant Index	(i) in respect of man day rates the relevant managerial and/or professional band of the HAY Index produced by The HAY Group Management Limited (Company No 763575) based on the financial provincial scales for systems staff in the managerial and professional bands as the case may be; and (ii) in respect of all other fees the U.K. All Items index of the Retail Prices Index as published by the Office for National Statistics (or its successor from time to time), or any official index replacing it; If any of indices referred to in (i) or (ii) above ceases to be published then a broadly equivalent index (as may be reasonably determined by Experian) will be used as a substitute;
Sanctions	As in force from time to time, any treaty, law regulation, decree, ordinance, order, decision, directive, policy, demand, request, rule or requirement imposed, administered or enforced from time to time by any Sanctions Authority: (a) relating to any economic, financial trade or other, sanction, restriction, embargo, import or

	export ban, prohibition on receipt or transfer of funds or assets or on performing services, or equivalent measure; or (b) directed at prohibiting or restricting dealings with Sanctions Restricted Person(s);
Sanctions Authority	Meaning any of: (a) the United Kingdom; (b) the European Union or any of its Member States; (c) the United States of America; and the respective governmental institutions and agencies of any of the foregoing in items (a) to (c) above;
Sanctions Restricted Person	Any person or entity: (i) included on the Consolidated List of Financial Sanctions Targets maintained by Her Majesty's Treasury; (ii) included on the Consolidated List of Persons, Groups and Entities subject to European Union Financial Sanctions; (iii) included on the Specially Designated National and Blocked Persons List maintained by the United States Office of Foreign Assets Control; (iv) included on any other list of a similar nature administered by a Sanctions Authority in respect of persons or entities with whom dealings are prohibited and/or whose assets are blocked; (v) owned 50% or more of, if applicable in accordance with respective Sanctions, controlled by any person, entity or body appearing on any list referred to in items (i) to (iv);
Word or Expression	**Meaning**
Schedule	The schedule or schedules which describe the subject matter and specific terms relating to this Agreement
Scorecard	A statistical formula derived to aid decision making and any supporting material in relation to such formulae;
Services	The services as specified in the Schedule and all other services supplied by Experian to the Client under or in connection with this Agreement, including the provision and grant of licences in respect of any Experian Data and/or Experian Material;

Specification	Any document identified as a specification in the Schedule (as such document is updated by agreement between the parties from time to time), or if none, Experian's standard configuration for the Services from time to time;
Sub-processor	Any person (including any third party and any Experian Group Company but excluding an employee of Experian or any of its sub-contractors) appointed by or on behalf of Experian to process Personal Data on behalf of Experian in connection with the Agreement;
Term	The duration of this Agreement as determined in accordance with Clause 2.1;
Territory	The United Kingdom;
UK GDPR	the General Data Protection Regulation (1016/679), to the extent that and in the form that it is a requirement of English law from time to time;
User Access Device	Any identification code, username, password, digital certificate, web certificate or any other security device provided by Experian and used by the Client to access the Services.

Service Description:

Service 1. Initial Identity verification

Experian's Identity Verification service (KYC) Identity Verification will be integrated into OPG's existing solutions and business processes through our Identity and Fraud single API Crosscore platform for real-time processing.

This will be accomplished by validating the accuracy of the supplied details such as name, date of birth, and address, verifying the existence of the individual, and confirming that the presenter

of these details is the legitimate owner. This comprehensive process is commonly referred to as 'authentication.'

The solution employs a robust 3-dimensional approach to customer authentication. By leveraging the extensive data, spanning over 1 billion records within Experian databases, a thorough assessment of the customer's information is conducted, considering its breadth, depth, and quality of data. This service will enable our OPG to meet Anti-Money Laundering (AML) regulatory responsibilities.

Service 2: Knowledge based question ID verification.

The Experian Identity IQ (IIQ) solution will enable OPG to seamlessly enhance identity verification measures across contact channels, thereby reducing customer friction and increasing security. By leveraging knowledge-based authentication, our robust data capabilities provides customised strategies and generate randomised questions that only a genuine customer will be able to answer correctly and mitigates the risk of fraudulent activities.

The delivery of this solution employs a random question generation system, specifically through Experian's Identity IQ (IIQ) SOAP XML. This integration enables the incorporation of authentication functionality into existing services by accessing customer data from the Experian databases. The system currently offers approximately 95 different questions for selection, which can be tailored and configured, providing a versatile approach to questioning strategies.

Service 3: Fraud Checking Services

Experian Fraud Score:

Experian Fraud Score service delivered to OPG is a fraud identification service which assesses the fraud risk of an application or transaction, and then returns a fraud propensity score ranging from 0 - 1000 and Reason Codes which provide further insight into the reason behind the score. This score can then be used to help inform whether to approve, manually review or reject an application/transaction.

The Fraud score model is trained on real-world credit fraud feedback data, to identify potentially fraudulent interactions and the service performance is regularly monitored by Experian.

The Experian Fraud Score shall be integrated with customer business processes through our Identity and Fraud single API Crosscore platform for real-time processing.

Joint Schedule 11 (Processing Data)

Definitions

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

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

Status of the Controller

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

(a) "Controller" in respect of the other Party who is "Processor";

(b) "Processor" in respect of the other Party who is "Controller";

(c) "Joint Controller" with the other Party;

(d) "Independent Controller" of the Personal Data where the other Party is also "Controller",

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

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

4. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

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

(a) Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;

(B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

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

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;

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

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

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

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

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Personal Data Breach.

8. The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

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

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Personal Data Breach; and/or

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

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

(a) the Controller determines that the Processing is not occasional;

(b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

(c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

13. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

(a) notify the Controller in writing of the intended Subprocessor and Processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

14. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable

certification scheme (which shall apply when incorporated by attachment to the Contract).

16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

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

Independent Controllers of Personal Data

18. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

19. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

22. The Parties shall only provide Personal Data to each other:

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

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

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

23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

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

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

(i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

(ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

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

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

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

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

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

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

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

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

1.3 Annex 1 - Processing Personal Data

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

1.1.1.1 The contact details of the Relevant Authority's Data Protection Officer is: [REDACTED]

1.1.1.2 The contact details of the Supplier's Data Protection Officer is: [REDACTED]

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

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

Description	Details
Identity of Controller for each Category of Personal Data	Ministry of Justice is the data controller and the Supplier is the data processor.
Duration of the Processing	As per the Call-Off Start date to Call-Off Expiry date and to include the Call-Off Optional Extension Period of 12 months as referred to in the Call-Off Order Form (Contract – con_23861 Third Party Identification Verification Services) for this contract.
Nature and purposes of the Processing	As specified within Call-Off Schedule 20 (Call-Off Specification) of this Call-Off Order Form (Contract – con_23861 Third Party Identification Verification Services).

Type of Personal Data	● Initial ● First name ● Surname ● Date of Birth ● Gender ● House number ● Street ● Post Code ● Customer URN ● Passport number ● Driving Licence Number
Categories of Data Subject	OPG Customers – members of the public applying to register an LPA who require ID verification in line with the Powers of Attorney Act 2023
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	For the duration of the contract, and in accordance with the provisions in paragraph 18.4.8(Experian Amended terms) of the Call-Off Order form (Contract – con_23861 Third Party Identification Verification Services).

Annex 2 - Joint Controller Agreement – NOT APPLICABLE FOR THIS CONTRACT

1. Joint Controller Status and Allocation of Responsibilities

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

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

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

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

2. Undertakings of both Parties

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

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

(i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

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

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

(j) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

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

3. Data Protection Breach

1.1.3.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the

investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

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

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

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

4. Audit

1.1.4.1 The Supplier shall permit:

(a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy

and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

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

5. Impact Assessments

1.1.5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. ICO Guidance

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

7. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

1.1.7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

(a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

1.1.7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the

Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

1.1.7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

(a) if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

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

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

8. Termination

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

9. Sub-Processing

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

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the

Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

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

Call-Off Schedule 5 (Pricing Details)

[REDACTED]

Call-Off Schedule 9 (Security Requirements)

Definitions

In this Schedule, the following definitions shall apply and be supplemental to those in Joint Schedule 1 (Definitions):

"Accreditation"	the assessment of the Core Information Management System in accordance with Part C of this Schedule by the Buyer or an independent information risk manager/professional appointed by the Buyer, which results in an Accreditation Decision;
"Accreditation Decision"	is the decision of the Buyer, taken in accordance with the process set out in Paragraph 4 of Part C of this Schedule, to issue the Supplier with a Risk Management Approval Statement or a Risk Management Rejection Notice in respect of the Core Information Management System;
"Accreditation Plan"	the Supplier's plan to attain an Accreditation Approval Statement from the Buyer, which is prepared by the Supplier and Approved by the Buyer in accordance with Part C of this Schedule;
“Anti-Malicious Software”	Software that scans for and identifies possible Malicious Software in the ICT Environment;
"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Services, the Sites, the Supplier System, and/or any information or data (including the Confidential Information and the Government Data) used by the Buyer, the Supplier or any

	Subcontractor in connection with this Call-Off Contract; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including copies of such information or data, used by the Buyer, the Supplier and/or any Subcontractor in connection with this Call-Off Contract; and/or (c) any part of the Supplier System ceasing to be compliant with the Certification Requirements, in each case as more particularly set out in the Security Requirements in Framework Schedule 1 (Specification) and the Order Form and the Security Requirements;
"Certification Requirements"	the requirements set out in Part E of this Schedule;
"CHECK Service Provider"	a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the ITHC Services required by the Paragraph 4.2 of Part C of this Schedule;
"CIMS Subcontractor"	a Subcontractor that provides or operates the whole, or a substantial part, of the Core Information Management System;
"Core Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Subcontractors to Process Government Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources) which the Buyer has determined in accordance with the Security Requirements;

General Security Requirements	the Security Requirements that shall apply to any Supplier and / or Subcontractor that processes Personal Data;
"Higher Risk Subcontractor"	a Subcontractor that Processes Government Data, where that data includes either: (a) the Personal Data of 1000 or more individuals in aggregate during the period between the Call-Off Start Date and the End Date; or **(b)** Special Category Personal Data, other than information about the access or dietary requirements of the individuals concerned;
"IT Health Check" (ITHC)	has the meaning given Paragraph 4.2 of Part C of this Schedule;
Incident Management Process	is the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Government Data, the Buyer, the Services and/or users of the Services and which shall be prepared by the Supplier in accordance with Paragraph 13.2 of Part A of this Schedule and as set out by the Supplier and Approved by the Buyer within the template set out in Section 23 of Appendix 1 of this Schedule;
"Information Assurance Assessment"	is the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Part B of this Schedule in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by

	the Supplier using the template set out in Appendix 1 of this Schedule;
"Information Management System"	the Core Information Management System and the Wider Information Management System;
"Information Security Approval Statement"	a notice issued by the Buyer which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that the Buyer: (i) is satisfied that the identified risks have been adequately and appropriately addressed; (ii) the Buyer has accepted the residual risks; and (iii) the Supplier may use the Information Management System to Process Government Data;
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"Medium Risk Subcontractor"	a Subcontractor that Processes Government Data, where that data (a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the Call-Off Start Date and the End Date; and (b) does not include Special Category Personal Data, other than information about the access or dietary requirements of the individuals concerned;
"Required Changes Register"	is a register which forms part of the Risk Management Documentation which records each of

	the changes that the Supplier has agreed with the Buyer to be made to the Core Information System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in the following Paragraphs within: ● 1.3 of Part B; ● 4 of Part C; ● 3 of Part D; together with the date on which each change shall be implemented and the date on which each change was implemented;
"Risk Management Approval Statement"	a notice issued by the Buyer which sets out the information risks associated with using the Core Information Management System and confirms that the Buyer is satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Buyer;
"Risk Management Documentation"	is the information and supporting documentation that the Supplier develops and provides to the Buyer when completing section 11 of the Security Management Plan;
"Risk Management Reject Notice"	has the meaning given in Paragraph 4.8.2;
“Security Management Plan”	comprises all information required from the Supplier in order to demonstrate compliance with the Security Requirements that must be presented in the templates set out in Appendix 1;

Security Requirements	the security requirements that the Supplier and each Subcontractor must comply with during the Contract Period as set out in the this Schedule;
"Security Test"	has the meaning given Paragraphs 4 in Part C and Part D of this Schedule;
Security Working Group	the meeting led by the Buyer (or their agent) with the Supplier to discuss the Security Management Plan and any risks, issues and controls the Supplier has put into place to ensure they are delivering the Security Requirements. The timing, required attendees and periodicity of the meetings will be defined by the Buyer during implementation, but should be no less than quarterly and should include the Supplier's Staff with the relevant expertise;
"Special Category of Personal Data"	the categories of Personal Data set out in Article 9(1) of GDPR;
"Statement of Information Risk Appetite"	the document that sets-out the type and level of risk that the Buyer is prepared to accept;
"Subcontractor Security Requirements"	any Security Requirements that must be delivered by Subcontractors;
"Vulnerability Correction Plan"	has the meaning given in Paragraph Part C Paragraph 4.3.3.1 of this Schedule;
"Wider Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Subcontractors to Process Government Data which have not been determined by the Buyer to form part of the Core Information Management System together with the associated information management system (including organisational

	structure, controls, policies, practices, procedures, processes and resources).

Part A Introduction

This Schedule sets out:

the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Call-Off Contract to ensure the security of Government Data, the Services and the Information Management System;

the Certification Requirements applicable to the Supplier and each of those Subcontractors which Processes Government Data;

the Security Requirements with which the Supplier must comply, which are dependent upon the applicable Lot(s) awarded to the Supplier under the Framework Contract;

the tests which the Supplier shall conduct on the Information Management System during the Term;

the Supplier's obligations to:

return or destroy Government Data on the expiry or earlier termination of this Call-Off Contract; and

prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in Paragraph 8; and

report Breaches of Security to the Buyer.

the applicable Tier of Security Requirements required to be complied with by the Supplier are summarised in Table 1 below:

Table 1:

Tier	Lot	Summary Security Requirements	Certification Requirements
1.	1	<u>General Security Requirements (Part B) plus PSC Accreditation (Part C)</u> The Supplier is also required to: a) ensure that terms and conditions no less onerous than those outlined in Part D of this Schedule are also flowed down within it's Subcontracts with Subcontractors; b) ensure that it's Subcontractors comply with the Security Requirements; and c) provide all documentation relating to the Subcontractors delivery of the Security Requirements including the Subcontractors Security Management Plans, to the Buyer immediately upon written request .	ISO 27001:2017 and Cyber Essentials (CE) + and PCI-DSS
2.	5, 6, 7, 20	<u>General Security Requirements (Part A) plus PSC Assurance (Part D) for Lot 20</u> The Supplier is also required to:	ISO 27001:2017 and CE+ and PCI-DSS

		a) ensure that terms and conditions no less onerous than those outlined in Part D of this Schedule are also flowed down within it's Subcontracts with Subcontractors; b) ensure that it's Subcontractors comply with the Security Requirements; and c) provide all documentation relating to the Subcontractors delivery of the Security Requirements including the Subcontractors Security Management Plans, to the Buyer immediately upon written request.	
3.	2, 3, 8, 9, 10, 11, 12, 13, 14	General Security Requirements (Part B)	ISO 27001:2017 and CE+
4.	4, 15, 16, 17, 18, 19	General Security Requirements (Part B) when handling Personal Data, otherwise N/A	CE

Principles of Security

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

the Sites;

the Supplier System;

the Information Management System, Core information Management System and Wider Information Management System, as applicable; and

the Services.

Notwithstanding the involvement of the Buyer in assessing the arrangements which the Supplier shall implement in order to ensure the security of the Government Data and the Information Management System, the Supplier shall be, and shall remain, responsible for:

the security, confidentiality, integrity and availability of the Government Data whilst that Government Data is under the control of the Supplier or any of its Subcontractors; and

the security of the Information Management System.

The Supplier shall:

comply with the Security Requirements in this Schedule; and

ensure that each Subcontractor that Processes Government Data complies with the Subcontractor Security Requirements in this Schedule.

The Supplier shall provide the Buyer with access to Supplier Staff responsible for information assurance to facilitate the Buyer's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.

The Buyer may at its sole discretion appoint an agent to act on it's behalf with regards to its engagement with the Supplier regarding the Security Requirements.

Part B General Security Requirements

1. The Security Management Plan

1.1 The Security Management Plan includes details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Buyer responsibilities which must be completed in order for the Supplier to receive a Risk Management Approval Statement.

1.2 The Supplier shall complete the Security Management Plan Template (Appendix 1) detailing how they will deliver the Security Requirements and the necessary information required for the applicable Tier(s) for the Lot(s) awarded to the Supplier. Any element that does not apply or only partially applies should be explained within the Template. If a Supplier is delivering Services in respect of more than 1 Lot, it must complete a separate Security Risk Management Template for each Lot.

1.3 Where there has been a Variation or Change to the Services which affects any aspect of the Security Requirements, CCS and the relevant Buyers must be notified immediately in writing of this fact and the extent of its effect or believed effect on the

Security Requirements and / or the Tier of the Security Requirements that the Supplier should apply to the Service (actual or potential).

1.4 The Supplier shall complete the Security Management Plan to demonstrate and document how they comply with the Security Requirements. A draft Security Management Plan shall be made available to the Buyer prior to the Call-Off Contract Effective Date unless already Approved by the Buyer.

1.5 The Security Management Plan should be provided to the Buyer in accordance with the Buyer's requirements and as set out within the Implementation Plan, but in any case, unless already Approved by the Buyer, this should be prior to the Service Effective Date.

2. **Security Classification of Information**

2.1 If the provision of the Services requires the Supplier to Process Government Data which is classified as: OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

3. **End User Devices**

3.1 The Supplier shall ensure that any Government Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Buyer, except where the Buyer has already Approved a suitable alternative arrangement.

3.2 The Supplier shall ensure that any device which is used to Process Government Data meets all of the Security Requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security

3.3 The Supplier must ensure that their EUD's require all Supplier Staff to authenticate themselves before gaining access to the device. All the Supplier's EUD's must encrypt all data at rest using a reputable full disk encryption solution that has been formally assured through a recognised certification process agreed with the Buyer, except where the Buyer has already Approved a suitable alternative arrangement. The Supplier's EUD's must be configured to automatically lock the screen after a period of inactivity and this must be agreed with the Buyer in writing.

4. **Location of Government Data**

4.1 The Supplier shall not and shall procure that none of its Subcontractors Process Government Data outside the UK without the Approval of the Buyer, which may be subject to conditions and that it shall comply with Joint Schedule 11 (Processing Data.

5. **Vulnerabilities and Corrective Action**

5.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Government Data.

5.2 The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability.

5.3 The Supplier shall utilise scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:

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

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

5.4 Subject to Paragraph 5.5, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:

5.4.1 7 days after the public release of patches for those vulnerabilities categorised as 'Critical';

5.4.2 30 days after the public release of patches for those vulnerabilities categorised as 'Important'; and

5.4.3 60 days after the public release of patches for those vulnerabilities categorised as 'Other'.

5.5 The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph 5.4 shall be extended where:

5.5.1 the Supplier can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 5.4 if the vulnerability becomes exploitable within the context of the Services;

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

5.5.3 the Buyer Approves to a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan; or

5.5.4 the Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Contract Period, unless otherwise Approved by the Buyer. All COTS Software should be no more than N-1 versions behind the latest software release.

6. Networking

6.1 The Supplier shall ensure that any Government Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected

enterprise network) or to a mobile device shall be encrypted when transmitted using TLS version 1.2 as a minimum.

7. Personnel Security

7.1 All Supplier Staff shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.

7.2 The Buyer and the Supplier shall review the roles and responsibilities of the Supplier Staff who will be involved in the management and/or provision of the Services in order to enable the Buyer to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Government Data or data which is classified as OFFICIAL-SENSITIVE.

7.3 The Supplier shall not permit Supplier Staff who fail the security checks required by Paragraphs 7.1 and 7.2 to be involved in the management and/or provision of the Services except where the Buyer Approves the involvement of the named individual in the management and/or provision of the Services.

7.4 The Supplier shall ensure that Supplier Staff are only granted such access to Government Data as is necessary to enable the Supplier Staff to perform their role and to fulfil their responsibilities.

7.5 The Supplier shall ensure that Supplier Staff who no longer require access to the Government Data (e.g. they cease to be employed by the Supplier or any of its

Subcontractors), have their rights to access the Government Data revoked within 1 Working Day

8. Identity, Authentication and Access Control

8.1 The Supplier shall operate an access control regime to ensure:

8.1.1 all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and

8.1.2 all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

8.2 The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require to perform the Services under the Contract.

8.3 The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such records available to the Buyer on request.

9. Audit and Protective Monitoring

9.1 The Supplier shall collect audit records which relate to security events in the Core Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Core Information Management System, to enable the identification of (without limitation) changing access trends, any unusual

patterns of usage and/or accounts accessing higher than average amounts of Government Data.

9.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the Core Information Management System.

9.3 The retention periods for audit records and event logs must be agreed with the Buyer and documented in the Security Management Plan.

10. Secure Architecture

10.1 The Supplier shall design the Core Information Management System in accordance with:

10.1.1 the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main;

10.1.2 the NCSC "Bulk Data Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main ; and

10.1.3 the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

11. Malicious Software

11.1 The Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Information Management System which may Process Government Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.

11.2 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 Government Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

11.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 11.1 shall be borne by the Parties as follows:

11.3.1 by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when the Data was provided to the Supplier, unless the Buyer had instructed the Supplier to quarantine and check the data for Malicious Software and the Supplier had failed to do so, and

11.3.2 by the Buyer, in any other circumstance.

12. Data Destruction or Deletion

12.1 The Supplier shall:

12.1.1 prior to securely sanitising any Government Data or when requested the Supplier shall provide the Buyer with two copies of all Buyer Data in an agreed open format;

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

12.1.3 securely erase in a manner agreed with the Buyer any or all Government Data held by the Supplier when requested to do so by the Buyer;

12.1.4 securely destroy in a manner agreed with the Buyer all media that has held Government Data at the end of life of that media in accordance with any specific

requirements in this Call-Off Contract and, in the absence of any such requirements, as agreed by the Buyer in writing; and

12.1.5 implement processes which address the CPNI and NCSC guidance on secure sanitisation.

13. Breach of Security

13.1 If either Party becomes aware or reasonably suspects of a Breach of Security it shall notify the other in accordance with the Incident Management Process.

13.2 The Incident Management Process shall, as a minimum, require the Supplier to do the following upon it becoming aware of a Breach of Security or attempted Breach of Security:

13.2.1 immediately take all reasonable steps necessary to:

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible;

(c) apply a tested mitigation against any such Breach of Security; and

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

13.2.2 as soon as reasonably practicable and, in any event, within twelve (12) hours following the Breach of Security or attempted Breach of Security, the Supplier must provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis as required by the Buyer.

13.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Subcontractors and/or all or any part of the Information Management System, with this Call-Off

Contract, then such remedial action shall be undertaken and completed at no additional cost to the Buyer.

14. Security Monitoring and Reporting

14.1 The Supplier shall:

14.1.1 monitor the delivery of assurance activities;

14.1.2 maintain and update the Security Management Plan in accordance with Paragraph 1;

14.1.3 agree a document which presents the residual security risks to inform the Buyer's decision on whether or not to give Approval to the Supplier to Process, store and transit the Government Data;

14.1.4 monitor security risk impacting upon the operation of the Service;

14.1.5 report Breaches of Security in accordance with the approved Incident Management Process; and

14.1.6 agree with the Buyer the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Buyer within 30 days of the Start Date of this Call-Off Contract.

Part C Accreditation requirements

1. **This Part sets out:**

1.1 The Accreditation arrangements that the Supplier must implement and comply with when providing the Services and performing its other obligations under this Call-Off Contract. These are required to ensure the security of the Government Data, the ICT Environment, the Services and the Information Management System, which are in

addition to the requirements set-out in Parts A, B and E and Appendix 1 and 2 of this Schedule.

1.2 To facilitate 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.

1.3 The Supplier shall provide access to the Supplier Staff responsible for information assurance and the Buyer shall provide access to its Personnel responsible for information assurance, at reasonable times upon reasonable written notice.

2. **Information Management System**

2.1. The Information Management System comprises the Core Information Management System and the Wider Information Management System.

2.2. The Buyer shall be responsible for determining the boundary between the Core Information Management System and the Wider Information Management System. In order to enable the Buyer to make such determination, the Supplier shall provide the Buyer with such documentation and information that the Buyer may reasonably require regarding any information assets, ICT systems and/or Sites which will be used by the Supplier or any Subcontractor to Process Government Data together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources). The Buyer shall notify the Supplier, as soon as reasonably practical following the receipt of such documentation and information, of its decision regarding the component parts of the Core Information Management System and its boundary with the Wider Information Management System.

2.3. The Supplier shall reproduce the Buyer's decision as a diagram documenting the Core Information Management System, the Wider Information Management system and the boundary between the two. This diagram shall form part of the Security Management Plan.

2.4. Any proposed change to the component parts of the Core Information Management System or the boundary between the Core Information Management System and the

Wider Information Management System shall be notified and processed in accordance with Clause 24 of the Core Terms (Changing the contract).

3. **Statement of Information Risk Appetite and Security Requirements**

3.1. The Supplier acknowledges that the Buyer has provided and the Supplier has received a statement of information risk appetite for the Supplier System and the Services ("**Statement of Information Risk Appetite**").

3.2. The Buyer's Security Requirements in respect of the Core Information Management System shall be set out in Appendix 1 (below).

4. **Accreditation of the Core Information Management System**

4.1. The Core Information Management System shall be subject to Accreditation in accordance with this Paragraph 4.

4.2. The Supplier acknowledges that the purpose of Accreditation is to ensure that:

4.2.1. the Security Management Plan accurately represents the Core Information Management System;

4.2.2. the Accreditation Plan, if followed, provides the Buyer with sufficient confidence that the CIMS will meet the requirements of the Security Requirements and the Statement of Risk Appetite; and

4.2.3. the residual risks of the Core Information Management System are no greater than those provided for in the Statement of Risk Appetite and Security Requirements.

4.3. The Accreditation shall be performed by the Buyer or by representatives appointed by the Buyer.

4.4. In addition to any obligations imposed by Call-Off Schedule 13 (Implementation Plan and Testing), the Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Call-Off Schedule 9 (Security Requirements), including any requirements imposed on Subcontractors, from the Call-Off Contract Start Date.

4.5. By the date specified in the Implementation Plan, the Supplier shall prepare and submit to the Buyer the risk management documentation for the Core Information

Management System, which shall be subject to approval by the Buyer in accordance with, Part B Paragraph 5 (the "**Security Management Plan**").

4.6. The Supplier must provide, by the date by which the Supplier is required to have received a Risk Management Approval Statement from the Buyer together with:

4.6.1. details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Buyer responsibilities which must be completed in order for the Supplier to receive a Risk Management Approval Statement pursuant to Paragraph 4.8.1.

4.6.2. a formal risk assessment of the Core Information Management System and a risk treatment plan for the Core Information Management System;

4.6.3. a completed ISO 27001:2013 Statement of Applicability for the Core Information Management System; the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Services, processes associated with the delivery of the Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to extent that it is under the control of or accessed the Supplier) and any IT, Information and data (including the Confidential Information of the Buyer and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services; and

4.6.4. unless such requirement is waived by the Buyer, proposed controls that will be implemented in respect of all aspects of the Services and all processes associated with the delivery of the Services, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Confidential Information of the Buyer and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Call-Off Contract or in connection with any system

that could directly or indirectly have an impact on that Information, data and/or the Services including:

4.6.4.1. the Required Changes Register;

4.6.4.2. evidence that the Supplier and each applicable Subcontractor is compliant with the Certification Requirements;

4.6.4.3. a Personal Data Processing Statement; and

4.6.4.4. the diagram documenting the Core Information Management System, the Wider Information Management System and the boundary between the two created under Paragraph 3.2.

4.7. To facilitate Accreditation of the Core Information Management System, the Supplier shall provide the Buyer and its authorised representatives with:

4.7.1. access to the Sites, ICT information assets and ICT systems within the Core Information Management System on request or in accordance with the Accreditation Plan; and

4.7.2. such other information and/or documentation that the Buyer or its authorised representatives may reasonably require, to enable the Buyer to establish that the Core Information Management System is compliant with the Security Management Plan.

4.8. The Buyer shall, by the relevant date set out in the Accreditation Plan, review the Security Management Plan and issue to the Supplier either:

4.8.1. a Risk Management Approval Statement which will then form part of the Security Management Plan, confirming that the Buyer is satisfied that the identified risks to the Core Information Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Buyer; or

4.8.2. a rejection notice stating that the Buyer considers that the identified risks to the Core Information Management System have not been adequately or appropriately addressed or the residual risks to the Core Information Management System have

not been reduced to the level anticipated by the Statement of Information Risk Appetite, and the reasons why (**"Risk Management Rejection Notice"**).

4.9. If the Buyer issues a Risk Management Rejection Notice, the Supplier shall, within 20 Working Days of the date of the Risk Management Rejection Notice:

4.9.1. address all of the issues raised by the Buyer in such notice;

4.9.2. update the Security Management Plan, as appropriate, and

4.9.3. notify the Buyer that the Core Information Management System is ready for an Accreditation Decision.

4.10. If the Buyer issues a two or more Risk Management Rejection Notices, the failure to receive a Risk Management Approval Statement shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.

4.11. Subject to Paragraph 4.10, the process set out in Paragraphs 4.9 shall be repeated until such time as the Buyer issues a Risk Management Approval Statement to the Supplier or terminates this Call-Off Contract.

4.12. The Supplier shall not use the Core Information Management System to Process Government Data prior to receiving a Risk Management Approval Statement.

4.13. The Supplier shall keep the Core Information Management System and Security Management Plan under review and shall update the Security Management Plan annually in accordance with this Paragraph 4 and the Buyer shall review the

Accreditation Decision annually and following the occurrence of any of the events set out in Paragraph 4.9.

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

4.14.1. a significant change to the components or architecture of the Core Information Management System;

4.14.2. a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;

4.14.3. a change in the threat profile;

4.14.4. a Subcontractor failure to comply with the Core Information Management System code of connection;

4.14.5. a significant change to any risk component; and/or

4.14.6. a significant change in the quantity of Personal Data held within the Core Information Management System.

4.15. Where the Supplier has previously Processed Personal Data that does not include Special Category Personal Data, it starts to Process Special Category Personal Data, other than data relating to accessibility or dietary requirements relating to an individual:

4.15.1. a proposal to change any of the Sites from which any part of the Services are provided; and

4.15.2. an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns; and

4.15.3. update the Required Changes Register and provide the updated Required Changes Register to the Buyer for review and Approval within 10 Working Days after the

initial notification or such other timescale as may be agreed with the Buyer.

4.16. If the Supplier fails to implement a change which is set out in the Required Changes Register by the date agreed with the Buyer, such failure shall constitute a material Default and the Supplier shall:

4.16.1. immediately cease using the Core Information Management System to Process Government Data until the Default is remedied, unless directed otherwise .by the Buyer in writing and then it may only continue to Process Government Data in accordance with the Buyer's written directions; and

4.16.2. where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Buyer and, should the Supplier fail to remedy the Default within such timescales, the Buyer may terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms

4.17. The Supplier shall review each Change request against the Security Management Plan to establish whether the documentation would need to be amended should such Change request be agreed and, where a Change request would require an amendment to the Security Management Plan, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change request for consideration and Approval by the Buyer.

4.18. The Supplier shall be solely responsible for the costs associated with developing and updating the Security Management Plan and carrying out any remedial action required by the Buyer as part of the Accreditation process.

5. Security Testing

5.1. The Supplier shall, at its own cost and expense:

5.1.1. procure testing of the Core Information Management System by a CHECK Service Provider (an "**IT Health Check**"):

5.1.1.1. prior to it submitting the Security Management Plan to the Buyer for an Accreditation Decision;

5.1.1.2. if directed to do so by the Buyer; and

5.1.1.3. once every 12 Months during the Call-Off Contract Period:

5.1.1.4. conduct vulnerability scanning and assessments of the Core Information Management System Monthly;

5.1.1.5. conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Subcontractors of a critical vulnerability alert from a supplier of any software or other component of the Core Information Management System to determine whether the vulnerability affects the Core Information Management System; and

5.1.1.5.1. conduct such other tests as are required by:

5.1.1.5.2. any Vulnerability Correction Plans;

5.1.1.5.3. the ISO27001 certification requirements;

5.1.1.5.4. the Security Management Plan; and

5.1.1.5.5. The Buyer following a Breach of Security or a significant change to the components or architecture of the Core Information Management System,

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

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

5.3. In relation to each IT Health Check, the Supplier shall:

5.3.1. agree with the Buyer the aim and scope of the IT Health Check;

5.3.2. promptly, and in any case no later than 10 Working Days, following receipt of each IT Health Check report, provide the Buyer with a copy of the IT Health Check report

5.3.3. in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

5.3.4. prepare a remedial plan for approval by the Buyer (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:

5.3.4.1. how the vulnerability will be remedied;

5.3.4.2. the date by which the vulnerability will be remedied;

5.3.4.3. the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer, include a further IT Health Check) to confirm that the vulnerability has been remedied;

5.3.4.4. comply with the Vulnerability Correction Plan; and

5.3.4.5. conduct such further Security Tests on the Core Information Management System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

5.4. The Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer.

5.5. The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to the Supplier's obligations under Paragraph 5.3, the Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable, and in any case no later than 10 Working Days, after completion of each Security Test.

5.6. The Buyer and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Service, the Information Management System and/or the Supplier's compliance with the Security Management Plan ("**Buyer Security Tests**"). The Buyer shall take reasonable steps to notify the Supplier prior to carrying out such Buyer Security Test to the extent that it is reasonably practicable for it to do so taking into account the nature and purpose of the Buyer Security Test.

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

5.8. The Buyer Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If a Buyer Security Test causes Supplier Non-Performance, the Buyer Security Test shall be treated as an Authority Cause for the purposes of Clause 5.1 of the Core Terms, except where the root cause of the Supplier Non-Performance was a weakness or vulnerability exposed by the Buyer Security Test.

5.9. Without prejudice to the provisions of Paragraph 5.3, where any Security Test carried out pursuant to this Paragraph 5 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the Core Information Management System and/or the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's Approval, the Supplier shall implement such changes to the Core Information Management System and/or the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible.

5.10. If the Buyer unreasonably withholds its Approval to the implementation of any changes proposed by the Supplier to the Security Management Plan in accordance with Paragraph 5.9 above, the Supplier shall not be deemed to be in breach of this Call-Off Contract to the extent it can be shown that such breach:

5.10.1. has arisen as a direct result of the Buyer unreasonably withholding its Approval to the implementation of such proposed changes; and

5.10.2. would have been avoided had the Buyer given its Approval to the implementation of such proposed changes.

5.11. For the avoidance of doubt, where a change to the Core Information Management System and/or the Security Management Plan is required to remedy non-compliance with the Risk Management Documentation, the Security Requirements and/or any obligation in this Call-Off Contract, the Supplier shall effect such change at its own cost and expense.

5.12. If any repeat Security Test carried out pursuant to Paragraph 5.3 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.

5.13. The Supplier shall, by 31 March of each Financial Year during the Call-Off Contract Period, provide to the Buyer a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:

5.13.1. the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this Call-Off Contract; and

5.13.2. the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.

6. Vulnerabilities and Corrective Action

6.1. In addition to the requirements within Part B, the Supplier shall:

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

6.1.2. promptly notify NCSC of any actual or sustained attempted Breach of Security;

6.1.3. ensure that the Core Information Management System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

6.1.4. ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Information Management System by actively monitoring the threat landscape during the Call-Off Contract Period;

6.1.5. pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Security Management Plan;

6.1.6. from the date specified in the Accreditation Plan and within 5 Working Days of the end of each subsequent Month during the Call-Off Contract Period, provide the Buyer with a written report which details both patched and outstanding vulnerabilities in the Core Information Management System, the elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report and any failure to comply with the timescales set out in Part B Paragraph 5.4 for applying patches to vulnerabilities in the Core Information Management System;

6.1.7. propose interim mitigation measures to vulnerabilities in the Core Information Management System known to be exploitable where a security patch is not immediately available;

6.1.8. remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Core Information Management System); and

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

6.2. If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Part B Paragraph 5.4, the Supplier shall immediately notify the Buyer.

6.3. If the Supplier fails to patch vulnerabilities in the Core Information Management System in accordance with Part B Paragraph 5.3, such failure shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.

PART D Assurance requirements

1. This Part D sets out the Assurance arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Call-Off Contract to ensure the security of the Government Data and the Information Management System.

1.1 The Supplier must comply with the Assurance arrangements in addition to the other Security Requirements as set out within Parts A and B and E of this Schedule and Appendix 1 (Security Management Plan).

2. **Information Security Approval Statement**

2.1 The Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Call-Off Schedule 9 (Security Requirements), including any requirements imposed on Sub-contractors from the Call-Off Start Date.

2.2 The Supplier may not use the Information Management System to Process Government Data unless and until:

2.2.1 the Supplier has procured the conduct of an ITHC of the Supplier System by a CHECK Service Provider in accordance with Paragraph 4; and

2.2.2 the Buyer has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 2.

2.3 The Supplier shall document in the Security Management Plan how the Supplier and its Subcontractors shall comply with the requirements set out in this Schedule and the Call-Off Contract in order to ensure the security of the Government Data and the Information Management System.

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

2.4.1 an Information Assurance Assessment;

2.4.2 the Required Changes Register;

2.4.3 the Personal Data Processing Statement; and

2.4.4 the Incident Management Process.

2.5 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within 20 Working Days of receipt and shall either issue the Supplier with:

2.5.1 an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Government Data; or

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

2.6 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Buyer's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Buyer for review within 10 Working Days or such other timescale as agreed with the Buyer.

2.7 The Buyer may require and the Supplier shall provide the Buyer and its authorised representatives with:

2.7.1 access to the Supplier Staff;

2.7.2 access to the Information Management System to Audit the Supplier and its Subcontractors' compliance with this Call-Off Contract;

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

2.7.4 assistance to the Buyer to establish whether the arrangements which the Supplier and its Subcontractors have implemented in order to ensure the security of the Government Data and the Information Management System are consistent with the representations in the Security Management Plan; and

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

3. **Compliance Reviews**

3.1 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.

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

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

3.2.2 a new risk to the components or architecture of the Service;

3.2.3 a vulnerability to the components or architecture of the Service which is classified '**Medium**', '**High**', '**Critical**' or '**Important**' in accordance with the classification methodology set out in Paragraph 5 of Part B to this Schedule;

3.2.4 a change in the threat profile;

3.2.5 a significant change to any risk component;

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

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

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

3.3 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Required Changes Register and submit the updated Required Changes Register the Buyer for review and Approval.

3.4 Where the Supplier is required to implement a change, including any change to the Information Management System the Supplier shall effect such change at its own cost and expense.

4. **Security Testing**

4.1 The Supplier shall, at its own cost and expense procure and conduct:

4.1.1 testing of the Information Management System by a CHECK Service Provider ("**ITHC**"); and

4.1.2 such other security tests as may be required by the Buyer; and

4.1.3 the Supplier shall complete all of the above security tests before the Supplier submits the Security Management Plan to the Buyer for review in accordance with Paragraph 3; and it shall repeat the ITHC not less than once every 12 Months during the Term and submit the results of each such test to the Buyer for review in accordance with this Paragraph.

4.2 In relation to each ITHC, the Supplier shall:

4.2.1 agree with the Buyer the aim and scope of the ITHC;

4.2.2 promptly, and no later than 10 Working Days, following the receipt of each ITHC report, provide the Buyer with a copy of the full report;

4.2.3 in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

(a) prepare a remedial plan for Approval by the Buyer (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the ITHC report:

(i) how the vulnerability will be remedied;

(ii) the date by which the vulnerability will be remedied; and

(iii) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer, include a further IT Health Check) to confirm that the vulnerability has been remedied;

(b) comply with the Vulnerability Correction Plan; and

(c) conduct such further tests on the Service as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

4.3 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Buyer.

4.4 If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique] that has the potential to affect the security of the Information Management System, the Supplier shall within days of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Buyer with a copy of the test report and:

4.4.1 propose interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available; and

4.4.2 where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Supplier System) within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

4.5 The Supplier shall conduct such further tests of the Supplier System as may be required by the Buyer from time to time to demonstrate compliance with its obligations set out this Schedule and the Call-Off Contract.

4.6 The Supplier shall notify the Buyer immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Paragraph 5 of Part B to this Schedule.

Part E Certification requirements

Certification Requirements

1. Supplier Requirements

1.1. The Supplier shall as applicable to the Lot and the associated Security Tier, ensure, at all times during the Call-Off Contract Period, that it is certified as compliant with:

1.1.1. ISO/IEC 27001:2013 by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

1.1.2. Cyber Essentials or Cyber Essentials PLUS as applicable to the Lot and Security Tier of the Service, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme), and shall provide the Buyer with a copy of each such certificate of compliance before the Supplier or the relevant Subcontractor (as applicable) shall be permitted to use the Core Information Management System to receive, store or Process any Government Data.

2. **Payment Card Industry Data Security Standard (PCI DSS) Compliance**

2.1. All Suppliers and / or Subcontractors that are a payment processor must be, and remain, appropriately certified according to the Payment Card Industry Data Security Standard requirements throughout the term of the Contract

2.2. Where the Supplier and / or Subcontractor intends to accept payments, restricted to at sale only, by debit/credit card the Supplier and / or Subcontractor must have either:

2.2.1. been certified by a Qualified Security Assessor [and Approved Scanning Vendor (as applicable)] as being compliant with the PCI DSS version 1.1;

2.2.2. completed an internal self-assessment and will adhere at all times to the terms of the PCI DSS and will notify the Client promptly in writing of any changes in the Contractor's certification.

2.3. The Supplier / Subcontractor must validate compliance in the manner deemed appropriate by the card scheme industry on an annual basis and provide the Buyer with written evidence of compliance annually.

2.4. The Supplier / Subcontractor will be responsible for any costs incurred to attain and maintain compliance with PCI DSS.

2.5. The Supplier / Subcontractor must meet all PCI DSS requirements, on a continuing basis, including but not limited to any subsequent versions of the PCI DSS.

2.6. The Supplier / Subcontractor must be responsible for the security of all cardholder Data in their possession and must protect data by the card scheme industry standard on an annual basis and provide the Buyer access hosted environment and data when necessary.

2.7. The Supplier / Subcontractor must notify the Buyer and the card scheme industry immediately if it knows or suspects that there has been, or will be, a breach of the security of Cardholder Data or of the PCI DSS.

2.8. The Supplier / Subcontractor must indemnify the Buyer, its subsidiaries, affiliates, officers, employees and agents from and against all actions, demands, costs, Losses, whatsoever incurred by it or them arising out of or in connection with the Supplier's non-compliance with, or breach of, the PCI DSS or breach of Cardholder Data security.

2.9. The Supplier / Subcontractor must cease taking payments, by Debit Card / Credit Card, on behalf of the Buyer in the event that the Supplier becomes non-compliant with, or suffers a breach of, the PCI DSS or breach of Cardholder Data security.

3. **Subcontractor Requirement**

3.1. Notwithstanding anything else in this Contract, a CMIS Subcontractor shall be treated for all purposes as a Key Subcontractor.

3.2. In addition to the obligations contained in Joint Schedule 6 (Key Subcontractors), the Supplier must ensure that the Key Subcontract with each CIMS Subcontractor.

3.3. contains obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under this Call-Off Schedule 9 (Security Requirements);

3.3.1. provides for the Buyer to perform Accreditation of any part of the Core Information Management System that the CIMS Subcontractor provides or operates which is not otherwise subject to Accreditation under this Call-Off Schedule 6 (Security Requirements).

3.4. The Supplier shall ensure that each Higher Risk Subcontractor is certified as compliant, and the Supplier shall provide the Buyer with a copy of each such certificate of compliance before the Higher-Risk Subcontractor shall be permitted to receive, store or Process Government Data, with either:

3.4.1. ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; or

3.4.2. Cyber Essentials PLUS, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme),

3.5. The Supplier shall ensure that each Medium Risk Subcontractor is certified compliant with Cyber Essentials, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme).

3.6. The Supplier shall notify the Buyer as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Subcontractor ceases to be compliant with the Certification Requirements and, on request from the Buyer, shall or shall procure that the relevant Subcontractor shall:

3.6.1. immediately ceases using the Government Data; and

3.6.2. procure that the relevant Subcontractor promptly returns, destroys and/or erases the Government Data in accordance with Security Requirements.

3.7. The Buyer may agree to exempt, in whole or part, the Supplier or any Subcontractor from the Certification Requirements. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

Appendix 1

Security Management Plan Template

[Guidance Note: This template shall be completed by the Supplier in accordance with the applicable Tier of Security Requirements for the particular Lots awarded]

This Security Management Template and all subsequent Annexes to be completed by the Supplier within 30 days of signature of the Call Off order.

DRS Call-Off Schedule 9 (Appendix 1)

Security Management Plan Template

[Lot/Service]

[Supplier Name]

Author:

Owner:

Date:
Version:

15. [Guidance Note: *The Supplier shall complete this Security Management Plan Template in as much detail as possible and if any provision does not apply to the Supplier, it must explain why.*]

1 Executive Summary

<This section should contain a brief summary of the business context of the Supplier System [including any Subcontractor system], any key Information Assurance controls, assurance work done, off-shoring considerations and significant residual risks that need acceptance by the Buyer.>

Call-Off Schedule 9 (Security Requirement)

1.1 List of Contents

Call-Off Schedule 9 (Security Requirement)

Crown Copyright 2021

1.1 Security Requirements Change History

Version Number	Date of Change	Change made by	Nature and reason for change

1.2 References, Links and Dependencies

This Security Management Plan Template relies upon the supporting information and assurance provided by the following documents:

ID	Document Title	Reference	Date
1.			
2.			
3.			

2 System Description

3 Background

< A short description of the project/product/system. Describe its purpose, functionality, aim and scope.>

4 Organisational Ownership/Structure

< Who owns the system, operates the system and the organisational governance structure. This should include how any ongoing security management is integrated into the project governance e.g. how a Security Working Group reports to the Buyer and Buyer governance *board as per their Call-Off Contract.>*

5 Information assets and flows

<The information assets processed by the system, which should include a simple high level diagram on one page, as well as a list of the type and volumes of data that will be processed, managed and stored within the Supplier System. If Personal Data is processed, please include the fields used such as name, address, department DOB, NI number etc. in Annex 1 of Joint Schedule 11 (Processing Data).>

6 System Architecture

<A description of the physical system architecture, to include the system management. A diagram will need to be included here>

7 Users

<A brief description of the system users, to include HMG users as well as any service provider users and system managers. If relevant, the security clearance level requirements of those users should be included.>

8 Locations

<Detail where the data assets are stored and managed from. If any locations hold independent security certifications (e.g. ISO27001:2013) these should be specified, as well as any off-shoring considerations.>

9 Test and Development Systems

<Include information about any test and development systems, their locations and whether they contain live system data.>

10 Key roles and responsibilities

<A brief description of the lead security roles such as that of the SIRO, IAO, Security manager, Accreditor >

11 Accreditation/Assurance Scope

<This section should describe the scope of the Accreditation/Assurance for the system (applicable to Tier 1 and Tier 2 Security Requirements). The scope of the assurance assessment should be clearly indicated, expressly including those components upon which reliance is placed but where assurance will not be undertaken, e.g. a cloud hosting service. A logical diagram should be inserted here along with a brief description of the components.>

12 Risk appetite

OPG's corporate risk appetite for information security is Opposed, meaning the avoidance of risk and uncertainty is a key objective.

13 Business impact assessment

< A description of the information assets and the impact of their loss or corruption (e.g. large amounts of Official Sensitive Personal Data the loss of which would be severely damaging to individuals, embarrassing to HMG and could make HMG liable to an Information Commissioner Office investigation) in business terms should be included. This section should cover the impact on loss of confidentiality, integrity and availability of the assets. The format of this assessment may be dependent on the risk assessment method chosen.>

14 Risk assessment

<The content of this section will depend on the risk assessment methodology chosen. It should contain a prioritised list of the output of the formal information risk using plain English language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks. >

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C2: Internet-facing IP whitelist C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	Very low

R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low
R3	Internal users could maliciously or accidentally alter bank details.	Medium-High	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance. C13. All changes to user information are logged and audited. C14. Letters are automatically sent to users home addresses when bank details are altered. C15. Staff awareness training	Low

15 Controls

<The controls listed above to mitigate the risks identified should be detailed. There should be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below.>

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC
C15	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part of ISO27001 certification

16 Residual risks and actions

<A summary of the residual risks which are likely to be above the risk appetite stated (above), after all controls have been applied and verified, should be listed with actions and timescales included.>

17 In-service controls

< This section should describe the controls relating to the information lifecycle, including development, testing, in-service, termination and on-going risk management and accreditation assurance. Details of any formal assurance requirements specified in the Contract such as

security CHECK testing or maintained ISO27001 certification should be included. This section should include as a minimum:

a) *information risk management and timescales and triggers for a review;*

b) *contractual patching requirements and timescales for the different priorities of patch;*

c) *protective monitoring arrangements to include how anomalous behaviour is identified and acted upon as well as how logging and auditing of user activity is done;*

d) *configuration and change management;*

e) *incident management;*

f) *vulnerability management;*

g) *user access management; and*

h) *data sanitisation and disposal.>*

18 Security Operating Procedures (SyOPs)

< If needed any SyOps requirements should be included and referenced here.>

19 Third Party Subcontractors/Suppliers/Products

< Please provide a table of any third party subcontractor/suppliers and products that you are using to deliver your Services for the Buyer. Please also include the location of where they are Processing or storing the Data and what function they are performing as well as how they comply with the contractual security requirements. >

20 Physical Security

<Please provide details of the building where the service will operate from and describe the procedures and security in place to control access to premises and any areas holding Buyer assets. Detail the measures such as construction of buildings used for handling Buyer assets, availability of lockable storage, procedures covering end of day/silent hours, key management, visitor controls. Also include details of any automated access controls, alarms and CCTV coverage and details of the maintenance schedule of these security controls.>

21 Major Hardware and Software and end of support dates

< Please complete a table listing the end of support dates for hardware and software products and components. For example:>

Name	Version	End of mainstream Support/Extended Support	Notes/RAG Status
Server Host	HP XXXX	Feb 2020/ March 2022	

22 Incident Management Process

<The Suppliers' process, as agreed with the Buyer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to CCS / the Buyer

and the process that will be undertaken to mitigate the incidents and investigate the root cause.>

23 Security Requirements for User Organisations

<Any security requirements for connecting organisations or departments should be included or referenced here.>

24 Required Changes Register

<The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually.>

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status
1	6.4	A new Third Party supplier XXXX will be performing the print capability.	Buyer's name	11/11/2018	Jul-2019	Open

25 Personal Data Processing Statement

<The Supplier shall complete Annex 1 of Joint Schedule 11 (Processing Data) detailing: (i) the types of Personal Data which the Supplier and/or its Subcontractors are Processing on behalf of the Buyer; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Subcontractors are Processing on behalf of the Buyer; (iii) the nature and purpose of such Processing; (iv) the locations at which the Supplier and/or its Subcontractors Process Buyer Data; and, (v) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Buyer Data against a Security Breach including a Personal Data Breach.>

-:-

26 Annex A: ISO27001 and/or Cyber Essential Plus certificates

<Any certifications relied upon should have their certificates included>

27 Annex B: Cloud Security Principles assessment

<A spreadsheet may be attached>

28 Annex C: Protecting Bulk Data assessment if required by the Buyer

<A spreadsheet may be attached>

29 Annex D: Latest ITHC report and Vulnerability Correction Plan

Appendix 2

ACCREDITATION - CORE INFORMATION MANAGEMENT SYSTEM

DIAGRAM

[Guidance Note: To be completed in discussions with Supplier]

The Core Information Management System Diagram and all subsequent Annexes to be completed by the Supplier within 30 days of signature of the Call Off order.

[REDACTED]

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Experian - SF Global Instance incl. Partner Portal (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your

agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Experian - SF Global Instance incl. Partner Portal:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: [REDACTED]

To advise Experian - SF Global Instance incl. Partner Portal of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at [REDACTED] and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address. If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from Experian - SF Global Instance incl. Partner Portal

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to [REDACTED] and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Experian - SF Global Instance incl. Partner Portal

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:
i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may; ii. send us an email to [REDACTED] and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to ‘I agree to use electronic records and signatures’ before clicking ‘CONTINUE’ within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Experian - SF Global Instance incl. Partner Portal as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Experian - SF Global Instance incl. Partner Portal during the course of your relationship with Experian - SF Global Instance incl. Partner Portal.