CALL OFF AGREEMENT Reference Number: RM3707 Front Office Counters Framework Agreement

This Call Off Agreement is dated _____ 2023

This Call Off Agreement is agreed between:

The Minister for the Cabinet Office as represented by Government Digital Service, whose offices are located at The White Chapel Building,10 Whitechapel High Street, London E1 8QS ("**Authority**")

and

the Contractor (being Post Office Limited)

(each a "**Party**" and, together, the "**Parties**").

This is a Call Off Agreement under the Single Supplier Framework Agreement for the provision of Front Office Counter Services and other Related Services (the "**Framework Agreement**") and has been agreed pursuant to Clause 2.2 of the Framework Agreement and the Call Off Process.

1. Call Off Term

1.1 The Call Off Term will begin on the date hereof and will continue for the initial term set out in Clause 2.11 of the Framework Agreement. The Parties agree that for the purposes of Clause 2.11 of the Framework Agreement, the Initial Term of this Call Off Agreement shall be three (3) years. For the avoidance of doubt, the provisions set out in Clause 2.1.1 of the Framework Agreement which permit extensions of up to three further years or longer shall not apply in respect to this Call off Agreement.

1.2 The Parties may extend the Call Off Term in accordance with Clause 57.2 of the Framework Agreement as varied by paragraph 1 of Annex 11 (Other Variations).

2. Terms of the Call Off Agreement

2.1 Subject to Clause 2.6 of the Framework Agreement, the terms of the Framework Agreement are expressly incorporated by reference into this Call Off Agreement, except as otherwise varied herein.

2.2 All words and expressions defined in the Framework Agreement shall have the same meaning and constructions when used in this Call Off Agreement unless expressly stated otherwise herein. In the event of any conflict between the definition of any word and/or expression as defined in the Framework Agreement and the definition of any word and/or expression as defined in this Call Off Agreement, then the definition of such word and/or expression as defined in this Call Off Agreement shall prevail. Any defined terms specific to this Call Off Agreement shall be set out at the start of the relevant Annex to this Call Off Agreement.

2.3 Subject to Clause 2.7 of the Framework Agreement, the Parties may agree to vary the terms of the Framework Agreement which are incorporated by reference into this Call Off Agreement, and all such variations shall be documented in Annex 11 (Other Variations) hereof.

2.4 The Contractor confirms that where it is aware that the implementation of this Call Off Agreement may affect other Services provided under the Framework Agreement it has, before the Effective Date of this Call Off Agreement, disclosed the same to the Authority, the Lead Authority and to all other affected Service Recipients.

3. Authority Requirements

3.1 The detailed Authority Requirements applicable to this Call Off Agreement are as set out in Annex 1 hereof.

4. Service Levels and Service Credits

4.1 The Service Levels and Service Credits applicable to this Call Off Agreement, which have been agreed by the Contractor and the Authority pursuant to the Call Off Process are as set out in Annex 2 (Service Levels and Service Credits) hereof. The provisions relating to Service Levels and Service Credits which have been amended as appropriate from Schedule 2.2 (Service Levels and Service Credits) of the Framework Agreement are as set out in Annex 2 (Service Levels and Service Credits) hereof.

5. Contractor Solution

5.1 The detailed Contractor Solution applicable to this Call Off Agreement (based upon the outline Contractor Solution in Schedule 4.1 (Contractor Solution) of the Framework Agreement) is as set out in Annex 3 (Contractor Solution) hereof.

5.2 If the Contractor identifies any material conflict between the Authority Requirements and the Contractor Solution the Contractor may notify the Authority and the Parties shall use their respective reasonable endeavours to resolve the conflict. If the conflict cannot be resolved to the Authority's satisfaction within 5 Working Days of such notice (or such longer period as the Parties may agree in writing) the Authority shall have the right to notify the Contractor that the Authority Requirements shall take precedence (in accordance with Clause 1.5 of the Framework Agreement).

6. Authority Responsibilities

6.1 The detailed Authority Responsibilities applicable to this Call Off Agreement are as set out in Annex 4 (Authority Responsibilities) hereof.

7. Implementation

7.1 The Detailed Implementation Plan shall be developed in accordance with Clause 4 (Implementation Plan) of the Framework Agreement and the applicable procedures in Schedule 6.1 (Implementation Plan) thereof. The Parties agree that there is no Outline Implementation Plan and that the Detailed Implementation Plan shall be developed without reference to such plan.

8. Charges and Invoicing

8.1 The Charges applicable to this Call Off Agreement (based upon the Charges in Schedule 7.1 (Charges and Invoicing) of the Framework Agreement and the Financial Model set out in Schedule 7.5 (Financial Model) of the Framework Agreement and agreed in accordance with Clause 2.12 of the Framework Agreement) are as set out in Annex 6 (Charges and Invoicing) hereof. The invoicing procedures applicable to this Call Off Agreement are as set out in Clause 20 (Charges and Invoicing) of the Framework Agreement and, amended as

appropriate from Schedule 7.1 (Charges and Invoicing) of the Framework Agreement, Annex 6 (Charges and Invoicing) hereof.

9. Financial Model

9.1 The detailed Financial Model applicable to this Call Off Agreement (based upon the Financial Model in Schedule 7.5 (Financial Model) of the Framework Agreement) is as set out in Annex 7 (Financial Model) hereof.

10. Governance

10.1 The governance applicable to this Call Off Agreement is as set out in Schedule 8.1 (Governance) of the Framework Agreement. The Parties acknowledge that they are bound by the procedures in Schedule 8.1 (Governance) of the Framework Agreement where either Party requests a reference to the Framework Board in accordance with that Schedule 8.1 (Governance).

11. Key Personnel

11.1 The Key Personnel applicable to this Call Off Agreement are as set out in Annex 8 (Key Personnel) hereof. Any change to Annex 8 (Key Personnel) shall be subject to Clauses 31.6 to 31.12 of the Framework Agreement.

12. Pensions

12.1 The pensions provisions and obligations applicable to this Call Off Agreement are set out in Annex 9 (Pensions) hereof.

13. Insurance Requirements

13.1 The insurance requirements applicable to this Call Off Agreement (based upon the template insurance requirements set out in Schedule 2.6 (Insurance Requirements) of the Framework Agreement) are set out in Annex 10 (Insurance Requirements) hereof.

14. Other Variations

14.1 Any other variations to the terms of the Framework Agreement incorporated by reference herein shall be agreed in accordance with Paragraph 2.3 of this Call Off Agreement and shall be documented in Annex 11 (Other Variations) hereof.

15. Step-In Rights

15.1 The provisions of Clause 63 (Step In Rights) of the Framework Agreement shall not apply under this Call Off Agreement except as may be agreed otherwise by the Authority and the Contractor from time to time pursuant to the Change Control Procedure.

16. Formation of Call Off Agreement

The execution of this Call Off Order Form by each of the Contractor and the Authority shall create a valid and legally binding contract comprising the Clauses of and Schedules to the Framework Agreement which are stated in Clause 2 (Contracting Capacity and Arrangements for Call Off Agreements) of the Framework Agreement to be incorporated into the Call Off Agreement as amended and supplemented by this Call Off Order Form.

17. Status of Postmasters

In this Call Off Agreement the Contractor's Postmasters shall be treated as:

17.1 Contractor Personnel for data protection and information security purposes and not as Sub-processors. Any activity undertaken by an employee of a Postmaster in relation to data shall be deemed to be activity undertaken by the Postmaster and such employees shall not be treated as Sub-contractors or Sub-processors; and

17.2 Sub-contractors for all other purposes under this Call Off Agreement.

18. Status of Yoti

The Parties agree that Yoti shall be appointed as a Material Sub-contractor for the purpose of the Framework Agreement and this Call Off Agreement and that (i) the Contractor shall promptly take such steps and agree such changes to the Framework Agreement with the Lead Authority as may be necessary to give effect to such appointment; and (ii) until such time as the appointment is formally made under the Framework Agreement, Yoti shall be deemed to be a Material Sub-contractor for the purpose of this Call Off Agreement with effect from the Effective Date.

SIGNED for and on behalf of **THE MINISTER FOR THE CABINET OFFICE** by	**SIGNED** for and on behalf of **POST OFFICE LIMITED** by
Signature	Signature
Name	Name
Position	Position
Date	Date

ANNEX 1 – AUTHORITY REQUIREMENTS

Contents

1. INTRODUCTION

Our mission is to build one fast, simple and secure way for people to access government services. The One Login product is replacing circa 180 ways to log in and 44 different ways to prove your identity with one single ubiquitous account and product suite.

In order to do this the Authority needs to provide a broad range of options that will support different user groups to successfully access government services. For user groups with photo ID, standard financial footprints and high digital literacy this is relatively straight forward.

However, One Login's success will not be measured by our ability to meet the needs of this group, it will be measured by our ability to provide an efficient digital service to people who have low or no digital skills, no photo ID and limited financial footprints because they don't own their own homes or have loans or credit cards.

With this in mind, One Login is developing a number of different offerings to increase inclusion for its service.

The Contractor's service is part of our inclusion strategy. The value of providing a face to face offline channel is primarily twofold:

1. To enable us to support a wide range of additional document sets quickly
2. To provide some support for low digital skilled users who have photo ID but need a little help.

One Login is a GMPP programme that is delivering both incrementally and at pace. It is leveraging a test and learn approach.

The Authority would like to work collaboratively with the Contractor. The Authority's intention is to increase the number of document types that can be used to support users to prove their identity thus increasing the inclusion of the One Login Product.

The Authority will need the Contractor to support further enhancing the inclusion of the face-to-face offline channel service to better support citizens who face barriers to proving their ID - e.g. via; improved access, additional documents that will support ID-challenged groups, and technical innovations to support Assisted Digital interactions in a cost-effective manner. Such developments shall be discussed with the Contractor and agreed changes managed through the Change Control Procedure.

Leveraging a face to face offline channel shift service is new to the Authority, therefore we want to start small, prove out some technical concepts and ameliorate some challenges. The Authority is proposing therefore to start with a limited set of documents for the initial phase (as set out in paragraph 5 of the Functional Requirements sub-section of the General Requirements section below), learn lessons from their inclusion and then add additional options over time as our understanding of user needs and behaviour grows over time.

Lot 1 enabling the following services:

1. face to face identity verification
2. face to face checking and sending of documents
3. face to face issuing of documents
4. face to face payment acceptance and refund services
5. face to face support for citizens applying for services using electronic devices (such as tablets)
6. Review and assess identity evidence against required standards, templates and biometric features
7. Other related services where customers may find face to face help useful

The ambition for the Front Office Counter Services is to support the Digital Identity Programme's Offline face-to-face channel shift verification journey, namely supporting citizens who cannot get verified via other channels to successfully verify themselves using an offline face-to-face channel.

The target state is for the face-to-face offline channel to be used by individuals who need it most, with other verification methods used in the first instance (i.e. online), supported by customer services. However, to design a truly inclusive Digital Identity service, the Authority must offer a face to face offline channel for users who would otherwise be excluded by the online routes (e.g. those with access needs, low digital skills, etc).

Capitalised terms and expressions used in this Annex 1 - Authority Requirements shall have the meanings given in Framework Schedule 1 (Definitions) and/or Attachment 1 (Definitions) to Annex 11 of this Call Off Agreement, unless otherwise defined herein.

Data Protection. The Authority anticipates that the Authority will be the Controller and the Contractor will be the Processor for the purposes of the Data Protection Legislation. The processing of Personal Data in connection with this contract will be governed by and carried out in accordance with clause 43 and Schedule 9.4 (Processing, Personal Data & Data Subjects) of the Framework Agreement.

2. ACCESSIBILITY

1. The Contractor shall ensure that identity verification services are made available in the agreed upon locations during standard branch opening hours.

2. The Contractor shall ensure that all Outlets used in the delivery of any services under this agreement remain compliant with the Equality Act 2010 (Equality Act). The Contractor shall align to the principles set out in the Public Sector Equality Duty pages on GOV.UK (www.gov.uk/government/publications/public-sector-equality-duty), which in summary aim to:

    1. Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act.

2. Advance equality of opportunity between people who share a protected characteristic and those who do not, and
3. Foster good relations between people who share a protected characteristic and those who do not.

The Equality Act also explains that advancing equality of opportunity involves having due regard for the need to:

1. Remove or minimise disadvantages suffered by people due to their protected characteristics.
2. Take steps to meet the needs of people with certain protected characteristics where these are different from the needs of other people, and
3. Encourage people with certain protected characteristics to participate in public life or in other activities where their participation is disproportionately low.

3. The Contractor shall collaborate with the Authority to help provide a service delivery model that meets these objectives and promotes equality during the contract term.

4. The Contractor shall advise customers on how to access the Authority's GOV.UK One Login services in accordance with these requirements. This may include re-directing them to the Authority's online services if beneficial to the user.

3. GENERAL REQUIREMENTS

The initial phase will cover the implementation of a face to face verification process for users with documents as specified in the Functional Requirements below. This phase will be considered complete once a volume of users determined to be material (circa 1,000+) have successfully verified through the face-to-face offline channel route.

Over the duration of this Call Off Agreement, The Authority anticipates the face to face offline channel verification to be delivered in a number of phases as we scale volumes, functionality and iterate provision in line with changing user needs and continuous improvement. Following the initial phase of integration, the Authority would expect to expand our offering to support new users. These changes will be handled in accordance with standard contractual variation procedures if required.

Later phases of development of the Face-to-Face offline channel verification process will gradually expand the total number of documents offered for in-person verification. This will aim to offer a comprehensive set of supported documents so as to cover the majority of the prospective users. The Authority will communicate any specific requirements to the Contractor on the inclusion of these additional document types (see Appendix 2) once a decision has been taken as to which documents should be supported. Furthermore, the Contractor will need to communicate the mechanisms and costs associated with adding any additional document types to the Authority. Changes related to the inclusion of additional documents will be handled in accordance with the Change Control Procedure.

Functional Requirements

Alongside the journey flow in Appendix 1, the Contractor Office must implement a solution which meets the following requirements:

1. Provide an endpoint for the creation of an identity verification session
2. Provide an endpoint for the retrieval of the Contractor's outlets offering identity verification when called using a UK postcode
3. Provide the Authority with formatted customer letters, including QR codes, to be shared with the user by the Authority following the creation of the session.
4. Provide the ability for the Authority to add an expiry date to the customer letter
5. For the initial phase (as set out above), accept only the following documents (with any changes to this document set being subject to the Change Control Procedure):
    1. NFC Chipped Passport
    2. Non-Chipped Passport (where MRZ is available only)

3. UK Driving Licence
4. Biometric Residence permit (BRP)
5. EU/EEA Driving Licence
6. EU/EEA National Identity Cards

6. Validate that the identity document presented:
    1. Is genuine, as per GPG45 relevant standards (to enable the Authority to map a GPG45 score)
    2. Matches the document named in the decision letter
    3. Is in date, as defined by:
        1. UK NFC Chipped Passport - within 18 months post expiry date
        2. Other NFC Chipped Passport - within expiry date
        3. Non-Chipped Passport (where MRZ is available only) – within expiry date
        4. UK Driving Licence - within expiry date
        5. Biometric Residence permit (BRP) - within expiry date
        6. EU/EEA Driving Licence - within expiry date
        7. EU/EEA National Identity Cards - within expiry date
7. Process user data in accordance with clause 43 and Schedule 9.4 (Processing, Personal Data & Data Subjects) of the Call Off Agreement.
8. Keep audit logs of the users interaction with the Contractor for a period as agreed with the Authority.
9. Persist a transaction tracing ID (“user_tracking_id”) through from the creation of the session through to identity verification and provision of session report to the Authority.
10. Embed error handling at all points in the service to allow for continuity of service should errors be encountered
11. Following identity verification, provide the Authority with a session report to include:
    1. Legible scans of the document
    2. A picture of the user. The image should be a minimum of 720p resolution and be usable for identity verification.
    3. A report on the checks carried out against the identity document, in compliance with Table One
    4. All data captured by the Contractor on the user
    5. Determination on the authenticity of the document
12. Must check other photo and non-photo identity documents in later phases, as identified by the Authority, as illustrated in Appendix 2 of this Annex. The Contractor must demonstrate the process by which new documents would be supported, the cost expected to support documents, and the timescales required to support these new documents. Requests for changes to the service including additional document types or verification shall be managed in accordance with the Change Control Procedure.

4. DIGITAL REQUIREMENTS

Alongside the journey flow in Appendix 1 of this Annex, the Contractor’s solution must include:

1. All service, support and operations related to the processing of Authority Data must be UK based. This extends to any sub-processors or ancillary activities provided by the Contractor and its contracted partners to support the customer journey and security of transactions. Any exceptions or variations must be subject to the Authority’s security team review and acceptance and must be detailed in Attachment 3 to Annex 11, Security Management Plan, Appendix 4.
2. The Service must record and issue to the Authority (in a format to be agreed) accurate analytics, including the below:
    1. Total number of users whose customer documents are scanned
    2. Total number of users who are able to complete the session (ie, bring the correct document, have the document scanned and have their picture taken)
    3. Total number of users unable to verify due to suspected fraud in security centre
    4. Total number of successful verifications
3. Deployments and planned/unplanned maintenance shall be as follows:
    1. Planned maintenance should be advertised to users and the Authority at least 5 days in advance of any service downtime, with an approximate resolution time shared

2. Planned maintenance, where possible, should occur outside of normal business hours
3. Deployments should not require any downtime or cause any session disruption

4. Service availability/performance shall be as follows:
    1. The service should be available 99.5% of the time during business hours. The Contractor must specify how they measure service availability. This should be assessed through the availability of the API for session configuration, results report retrieval and other endpoint interactions.
    2. Successful API responses (2XX, 3XX, 4XX) must be received within 2 seconds 99% of the time, and within 10 seconds 99.95% of the time.
    3. 5XX responses and timeouts must occur for no more than 0.05% of invocations, i.e. the service must encounter fatal internal errors during less than 0.05% of submissions
    4. The API service must be able to handle a sustained volume of 1tps, and a peak volume of 10tps over a 5 min period for session creation.
    5. The API service must be able to handle a sustained volume of 1tps, and a peak to 3tps over a 5 min period for session results and retrieval.
5. The Services UK Geographic Coverage shall be as follows:
    1. Support the required % coverage as specified by the Authority (being 85%) of the overall UK population having a Contractor's premises face to face verification within 10 miles
    2. The existing % coverage within each nation previously provided by the Contractor is sufficient for the first release, however in future the Buyer will look to extend coverage to meet 85% of the overall UK population (including all four nations) having the Contractor's premises offering face to face verification within 10 miles. The Authority reserves the right to amend coverage requirements, in particular to support rural areas, and will work with the Contractor to explore the feasibility of extending coverage in the relevant geographic areas as appropriate. Without prejudice to the overall 85% coverage requirement (as may be amended under the Change Control Procedure), all coverage requirements shall take into account the constraints of available outlets that are able to support the Service, and under no circumstances will the Contractor be specifically required to operate any additional outlets solely for carrying the Service. Any changes to the coverage requirements shall be managed in accordance with the Change Control Procedure.
6. The Services shall comply with the following fraud requirements:
    1. Provide suspected fraud reports and/or suspicious activity reports as soon as possible to the Authority (and whenever practicable no later than the end of normal business hours on the next Working Day following the relevant event) - even on partial journeys i.e. those that are terminated by the postmaster.
    2. All security centre session activity shall be processed as soon as practicable and in any event within 72 hours of the relevant notification session being created.
    3. Ensure no data loss on transfer between systems.
    4. Ensure Image data is available for 30 days.
    5. Ensure images are saved securely in line with the standards described in section 9.2.
    6. Grant the Authority's fraud analysts access to stored images
    7. Images given to sub-contractors/3rd parties shall not be used for improving algorithms
    8. Security centre personnel are trained to a high level to identify forged and counterfeit documents
    9. Ensure mitigations against insider threat are in place

5. COMPLIANCE

1. The Contractor shall, where requested by the Authority complete a compliance review which may include an audit of services rendered, performance of contractual obligations and compliance with the terms and conditions of the contract.

2. In the event of an outlet (or personnel working at an outlet) ability or integrity being compromised in any way, the Authority shall raise a service management incident to the Contractor. The Contractor will assess whether the outlet needs to cease trading the service.

3. The Contractor shall regularly assess and monitor the performance of Postmasters and/or individuals and address poor performance issues. Where appropriate, the Contractor shall take appropriate actions to improve the quality of services provision, without additional cost and/or affecting continuity of service.

4. The Contractor shall maintain the geographical requirements as set out in the requirements, unless expressly agreed otherwise in writing with the Authority.

5. The Contractor shall provide the Authority with the details of Contractor Personnel within five (5) Working Days upon request. Information may include, but is not limited to the following:

    1. List of Outlets being utilised.
    2. Confirmation that Contractor Personnel have the 'right to work in the UK', including supporting evidence.
    3. List of security clearances held by Contractor Personnel including supporting evidence.

6. The Contractor shall ensure the records of any Contractor Personnel, are kept up to date to reflect the validity of their security clearances and right to work in the UK. These records should be held in a secure manner and upon request shared with either the Authority within 5 Working Days. For avoidance of doubt, such records would not include any of the Contractor Postmasters' employees.

7. The Contractor must work in collaboration with the Authority to ensure that any outcomes from a Compliance Review are acted upon and done so in a time period determined by the Authority.

8. The Contractor shall have robust processes in place to enable changes to the Authority's processes to be implemented. The Contractor shall enact any reasonable changes within 8 weeks of notification.

9. The Contractor shall have in place a robust fraud risk assessment for each of the Authority's service areas as set out in these requirements, which the Contractor shall share with the Authority within 5 Working Days of receiving a request in writing.

10. The Contractor shall keep a regular review of the fraud risk assessment for each service area, identifying and sharing known risks with the Authority. Where appropriate the Contractor shall share solutions to mitigate the risks identified.

11. The Contractor shall have a robust risk management process, which is regularly reviewed to ensure that the Authority is not exposed to undue risk including (but not limited to) as a result of the delivery of other aspects of the Contractors Offices business/business model. Where a risk is identified which may expose the Authority to any form of risk this should be communicated within 5 Working Days or at a time frame agreed by the Authority.

12. Employees of subcontractors shall not keep notes or copy any information in relation to the citizens personal data unless expressly linked to the process agreed by the Authority.

13. The Contractor shall effectively and securely destroy any physical printed collateral / forms / documents at the request of the Authority within 5 Working Days.

6. TRAINING

1. The Contractor shall be responsible for the professional development, accountability and quality of the Contractor Personnel. Where any member of the Contractor Personnel is not directly employed, the Contractor shall still remain responsible for ensuring that they have the correct

level of professional development, training, and quality to perform their responsibilities in the performance of any contract under this agreement.

2. The Contractor shall have processes in place to ensure training can be mobilised to implement new services. This training must conform to the requirements of the Authority and be rolled out across the network of outlets that will be utilised in the delivery of the Authority services in a timely manner. Contract change management processes will be utilised where the Authority makes a change to their use of the service requiring changes to training provided.

3. The Contractor shall, upon notification of changes to an existing service, work with the Authority to amend any training and ensure the Contractor Personnel are adequately trained within 8 weeks of appointment.

4. The Contractor shall ensure that the training is effective, where possible using testing to provide assurance.

5. The Contractor shall ensure that all Contractor Personnel receive training on the Data Protection Legislation and evidence of this training must be maintained for the duration of the Call Off Agreement. This may be requested by the Authority, and must be supplied within 5 Working Days.

7. SECURITY

1. The Contractor shall ensure that (i) all Contractor Personnel are security cleared to the appropriate level as specified by the Authority prior to them undertaking work on this Call off Agreement; and (ii) all services involving the processing of Authority Data are provided from within the UK.

2. As a minimum the Contractor shall ensure that all Contractor Personnel have passed a security clearance to Baseline Personnel Security Standard (BPSS) or an equivalent of BPSS in accordance with the government baseline personnel security standard (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard). It will be the responsibility of the Contractor to ensure that this minimum standard is met throughout the duration of the Call Off Agreement.

3. The Contractor shall ensure that Contractor's Personnel are made aware of and comply with the Contractor's confidentiality obligations under clause 45 of the Framework Agreement.

4. The Contractor must maintain accurate records in a secure manner to evidence compliance with the vetting requirements and/or any additional requirements set out by the Authority during the term of this Call Off Agreement. These must be provided to the Authority upon request within 5 Working Days.

5. In line with government approved standards and industry best practice, the Contractor may be required to implement physical, technical, personnel and procedural security controls as part of a layered or defence in depth approach to security that effectively balances prevention, detection, protection and response. The Contractor shall be responsible for the costs of developing and implementing such controls, provided that if following the Effective Date there is a new or amended mandatory standard that solely impacts the Authority and/or this Call Off Agreement (and not any other customer or contract of the Contractor) the Parties shall discuss how the standard should be met and the treatment of the Contractor's costs.

6. The Authority may, on giving reasonable notice in writing, carry out an annual review of the Contractor's compliance with the Security Schedule to ensure appropriate physical security protections are in place to reduce the risk to the Authority and their assets.

7. The Contractor shall ensure that a robust Security Incident/Breach procedure is in place, which upon request of the Authority shall be provided in accordance with the Security Schedule.

8. The Contractor shall inform the Authority within 24 hours of any compromise to the Contractor's and/or Buyers' assets, including but not limited to data breaches in accordance with the Security Schedule.

9. The Contractor shall ensure that its BCDR process and that of its subcontractors do not breach UK GDPR or the Data Protection Act 2018.

10. The Services must be delivered as per the GDS Service Manual (e.g. agile delivery aligned to scrum methodology) or other methodologies as required.

11. The Contractor shall comply with the Security Schedule (subject to the deviations set out in Appendix 1 of Annex 3 (Contractor Solution)) and shall in addition:

    (a) provide a Security Management Plan for approval by the Authority within 20 days of the commencement of this Call Off Agreement; and

    (b) engage in security management reviews with the Authority as required.

8. NOT USED

9. SERVICE STANDARDS

1. This section describes the required standards that the Contractor shall be obligated to comply with as part of the delivery of this Call Off Agreement.

2. The Contractor shall at all times during the term of this Call Off Agreement, comply with the Standards and must be certificated in the following Standards by the end of the first contract year:

a) Service Management Standards

- ISO 9001 - Certified
- ISO 14001 - Certified

b) Information Security Management Standards

- ISO 27001: 2017 - Certified

3.The Authority shall not be liable for any costs of implementing these Standards and the full cost of implementation shall be borne by the Contractor.

10. MANAGEMENT INFORMATION

1. Notwithstanding the requirements set out in Framework Schedule 5 (Management Charges and Information), this section describes the additional mandatory Management Information, monitoring and data reporting requirements that the Contractor must fulfil as part of the delivery of the Call off Agreement.

2. The Authority may request data and reports on an ad hoc basis to assist with Parliamentary Questions (PQs). Where data and a structured report is available, the Contractor shall provide within one Working Day of request by the Authority the required data. Where a report is not available the Contractor shall provide the required data to the Authority within 72 hours. The Contractor shall provide the Authority with data in relation to the number of complaints received on a quarterly basis. This data must inform the Authority at a minimum about:
    1. total volume of complaints
    2. the volume upheld
    3. the volume which were considered unfounded
    4. the volume by service delivery
    5. volume by location

3. The Contractor, working together with the Authority, must be able to contribute to the effective measurement of change in user behaviour across various services. For example a methodology to measure a change in usage from paper applications to digital solutions.

4. The Contractor shall provide the Authority, with regular management information (weekly updates, at a minimum, from the outset) about, but not limited to:
    1. the volume of applications processed,
    2. the volume of declined applications (citizen)
    3. broken down by reason
    4. geographical location of usage
    5. number of outlets available
    6. utilisation per outlet
    7. journeys flagged as suspicious by:
        - type of fraud / document
        - time of fraud
        - location of fraud
        - action taken

5. The Contractor shall produce and provide to the Authority any requested tailored/non-standard Management Information reports as may be reasonably requested by the Authority from time to time which shall be provided free of charge, for example Equality and Diversity Monitoring.

6. The Contractor shall provide MI on the performance of the service via scheduled or ad hoc reports.

11. COMPLAINTS

This section describes the additional mandatory complaints procedures that the Contractor must fulfil as part of the delivery of this Call Off Agreement.

1. The Contractor shall have in place robust and auditable procedures for logging, investigating, managing, escalating and resolving complaints initiated by users, its representatives and/or its customers, employees and contractors. The procedure should allow for the identification and tracking of individual complaints from initiation to resolution.

2. A clearly defined complaints procedure is required which sets out timescales of the action that shall be taken and includes timescales of when matters shall be escalated.

3. The Contractor shall ensure that any complaints received directly from a user who are encountering problems whilst trying to use a service are dealt with as a matter of priority.

4. Complaints made by a user or the Authority should be acknowledged within 24 hours of the complaint being received by the Contractor. Thereafter updates on how the Contractor is proactively working to seek a resolution of the complaint should be made by the Contractor to the user or the Authority at regular intervals, until a satisfactory resolution has been agreed which is mutually acceptable to both parties. As a minimum, complaints shall be acknowledged within 24 hours, and where possible, the majority of complaints shall be satisfactorily resolved within 5 Working Days, or at time period in agreement with the Authority.

5. The Contractor shall provide comprehensive reports on all complaints to the Authority on a monthly basis or as agreed within this Call Off Agreement. These reports shall include the date of the complaint was received and resolved, complainant contact details, the nature of the complaint and actions agreed and taken to resolve the complaint.

6. The level and nature of complaints arising and proposed corrective action shall be reviewed by the parties periodically, as appropriate according to the numbers of complaints arising, and in any event at intervals of 3 months.

12. WHISTLEBLOWING

1. The Contractor shall throughout the term of this Call Off Agreement put in place, maintain and comply with a policy that enables Contractor Personnel to voice concerns in a responsible and effective manner, this includes where a Contractor Personnel member and other members of your organisation discovers information which they believe shows serious malpractice or wrongdoing within the organisation. The policy shall allow for this information to be disclosed internally without fear of reprisal, and there should be arrangements to enable this to be done independently of line management. The policy shall include:

    1. Details of The Public Interest Disclosure Act, which came into effect in 1999 and gives legal protection to employees against being dismissed or penalised by their employers as a result of publicly disclosing certain serious concerns.
    2. Details of a prescribed person or body if an individual feels they cannot go to their employer.

13. SOCIAL VALUE

1. Social Value legislation places a legal requirement on all public bodies to consider the additional social, economic and environmental benefits that can be realised for individuals and communities through commissioning and procurement activity, and, in Scotland, to deliver them. These benefits are over and above the core deliverables of Contracts. General information on the Social Value Act can be found here.

2. Recent guidance published in Procurement Policy Note 06/20 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/921437/PPN-06_20-Taking-Account-of-Social-Value-in-the-Award-of-Central-Government-Contracts.pdf) requires that Social value should be explicitly evaluated in all central government procurement rather than just 'considered as required under the Public Services (Social Value) Act 2012. Updated social value themes for public bodies can be found on this link.

3. The following Social Value priorities are intrinsic to the specification for this Call Off Agreement:
    1. Covid 19 Recovery
    2. Tackling economic inequality
    3. Fighting Climate Change
    4. Equal Opportunity
    5. Wellbeing

4. The Authority may identify further specific Social Value priorities based on the updated social value themes during a Call-Off Procedure.

5. The Contractor shall be prepared to provide delivery plans and reporting of impacts and performance of social value to buyers (e.g. method statements and KPIs), as may be required by the Authority.

APPENDIX 1 – LOT 1

1. The Contractor shall provide Front Office Counter Services throughout the United Kingdom via a network of outlets which provide face to face support to users. These services must be accessible in line with the mandatory requirements set out above.
2. The services the Contractor must be able to provide include, but are not limited to:

    1. face to face documentation checks
    2. face to face identification verification
    3. face to face issuing service

3. The Contractor should have a robust management process in place to deliver high volume requirements across the whole of the United Kingdom.

Documentation Checks - In Person

4. The Contractor shall provide a comprehensive face to face document checking service. This service will include, but is not limited to, the following requirements:

    1. To provide guidance in person on the general process and manage citizens expectations about the process in line with the Authority's guidance.

5. The Contractor shall be responsible for all administrative costs associated with the delivery of the document checking services.

6. The Contractor shall ensure that any documents provided in support of the forms are acceptable in accordance with the Authority's requirements.

7. Where necessary, the Contractor may make direct contact with the Authority (via a telephone or online) to resolve real time issues and seek guidance.

Documentation Checks - Digital

8. The Contractor shall provide a comprehensive face to face electronic document checking service. This service will include, but is not limited to, the following requirements:

    1. Face to face capture personal details on behalf of the citizen electronically. Electronically send this information to a format and schedule agreed by the Authority.

9. The Contractor shall ensure it has the capability to design, build and manage the requirement for the electronic transfer of data in accordance with the guidance provided by the NCSC on Security Design Principles (https://www.ncsc.gov.uk/collection/cyber-security-design-principles) and Using TLS to protect data (https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data). These shall be provided via standardised approaches, frameworks and languages for API integration (for example JSON/XML), but on occasion may require more bespoke solutions.

10. Where there are investment costs to deliver the Authority needs these will be agreed at Call Off Stage and be charged separately.

11. The Contractor shall ensure it has the technical expertise and capability to capture data in line with the Authority needs using its own IT infrastructure (including assistive technology such as tablets), including the reading of barcodes and/or QR as a form identification tool.

12. The Contractor shall be responsible for all administrative costs associated with the delivery of the digital document checking services, including service and maintenance costs for any system / IT requirements.

13. The Contractor shall ensure that any documents provided in support of the citizens forms are acceptable in accordance with the Authority's requirements.

Identity Checks

14. The Contractor shall provide a comprehensive face to face identity checking service, including the capability to check physical and digital identification documents. This service will include, but is not limited to, the following requirements:

1. face to face review of the citizens evidence of identity to ensure compliance with the Authority's requirements
2. To check for any potential fraudulent evidence as part of the Authority's
3. processes
4. To make copies of any evidence provided by the citizens in line with the Authority's requirements.
5. To provide guidance on the general process and manage citizens expectations about the process in line with the Authority's guidance.

15. The Contractor shall ensure that all validation and verification checks are compliant with the Good Practice Guidance 45 (www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual) or any updated guidance set out on behalf of the public sector. The Contractor shall ensure it has the capability to work with the Authority to align to their needs, including the necessary confidence level set out in the GPG45 (Low - Very High) and their respective processes.

16. The Contractor shall have the capacity to manage these checks, which may take up to 15 minutes (longer in some instances) to process across the network of outlets.

17. The Contractor shall have the capacity to review and check the validity of a multitude of documents, not limited to the following documents, as per agreed scope of initial phase

    1. NFC Chipped Passport
    2. Non-Chipped Passport (where MRZ is available only)
    3. UK Driving Licence
    4. Biometric Residence Permit (BRP)
    5. EU/EEA Driving License
    6. EU/EEA National Identity Cards

18. The Contractor shall have the capability to integrate digital solutions such as real time eligibility checks into their processes and service offering. Requests to add documents for verification or additional checks to the process shall be managed in accordance with the Change Control Procedure.

19. The Contractor shall verify the identification of the citizen by reviewing the evidence/documents provided by ensuring they are genuine and correspondent to the citizen in line with the Authority's guidance.

20. The Contractor shall have robust measures in place to identify where there is a risk of fraud, and appropriate measures to escalate any incidents to the Authority to mitigate the risk of fraud.

APPENDIX 2 – MVP SERVICE DESIGN

1. Prior to attending the outlet the user will have carried out the following:
   a. Creation of a GOV.UK Account
   b. Chosen a route for identity verification requiring an face to face identity check
   c. Affirmed that they carry one of the documents (which once checked will meet the Buyer's identity needs) within the appropriate validity window, as agreed in section 3:
      1. NFC Chipped Passport
      2. Non-Chipped Passport (where MRZ is available only)
      3. UK Driving Licence
      4. Biometric Residence Permit (BRP)
      5. EU/EEA Driving Licence

6. EU/EEA National Identity Cards

d. Choose which of the above documents they will carry to the Contractor's outlets.
e. Provided their full name, full postal address, date of birth and email/SMS contact details
f. Selected outlet near them to have their documents verified in
g. Confirmed that they will attend the outlet for face to face verification

2. A request will be made from the Buyer to the Contractor to create a session and customer letter. This request will include, at a minimum:
   a. A correlation/tracing ID ("user_tracking_id")
   b. The name of the user
   c. The date of birth of the user
   d. The address of the user
   e. The document (or, in future, documents) the user will be bringing to the Contractor premises
   f. An indication that a customer letter should be shared with the Authority (Ie, "IN STRUCTIONS_EMAIL_REQUESTED" enabled)
   g. The Contractor that they will be attending to verify their identity documents

3. The Contractor Personnel will confirm that a session has been created.

4. The Contractor's Personnel will confirm to the Authority that a customer letter is available for the user

5. the Authority will retrieve the customer letter and forward to the user internally

6. Later, the user will visit their chosen outlet which offers identity verification with their customer letter. They should go through the below process in a local branch:
   a. The Contractor Personnel must scan the QR code contained in the user's letter
   b. The Contractor Personnel must validate that the user has brought the correct docu ment, as per their customer letter
   c. The Contractor Personnel must validate that the picture in the identity document matches the user
   d. The Contractor Personnel must check that the document is valid and genuine
   e. The Contractor Personnel must take a picture of the user
   f. The Contractor Personnel must take a picture of the user's identity document
   g. (If the user has a passport) The Contractor Personnel must perform an NFC scan of the user's identity document
   h. If the documents do not meet the required standard (through fakery, fraudulence, etc) then the user should be informed and the session should be ended.in this scenario, data must be provided to the Authority on the reason the session was ended

7. Once the user's identity check is completed by the Contractor Personnel, the Contractor Personnel must upload the doc images and photograph and forward this session data onto the Contractor's Security Centre to complete additional document and face match checks, when required by the Authority.

8. The Contractor's Security Centre must evaluate the user's identity document submission, and then notify the Authority of the outcome through sharing a single session report to include the scanned identity document and image of the user, along with confirmations of the process carried out to validate the user's identity document.

APPENDIX 3 – ADDITIONAL DOCUMENTATION REQUIREMENTS

Beyond Phase One Documentation Assessment Criteria
The below list records the different pieces of evidence that may be required in the future. Should support for these documents be required, the Authority will provide sufficient notice via the Change Control Procedure.

- Council Regulation (EC) No 2252/2004
- Northern Ireland Voters Card
- US passport card
- Retail bank/credit union/building society current account
- Student loan account
- Bank credit account (credit card)
- Non-bank credit account (including credit/store/charge cards)
- Bank savings account
- Buy to let mortgage account
- Digital tachograph card
- Armed forces ID card
- Proof of age card issued under the Proof of Age Standards Scheme (containing a unique reference number)
- Secured loan account (including hire purchase)
- Mortgage account
- 2006/126/EC
- Firearm Certificate
- DBS Enhanced Disclosure Certificate
- HMG issued convention travel document
- HMG issued stateless person document
- HMG issued certificate of travel
- HMG issued certificate of identity
- Birth Certificate
- Adoption Certificate
- UK asylum seekers Application Registration Card (ARC)
- National 60+ bus pass
- Unsecured personal loan account (excluding pay day loans)
- An education certificate gained from an educational institution regulated or administered by a Public Authority (e.g. GCSE, GCE, A Level, O Level)
- An education certificate gained from a well recognised higher
- educational institution
- Residential property rental or purchase agreement
- Proof of age card issued under the Proof of Age Standards Scheme (without a unique reference number)
- Police warrant card
- Freedom pass
- Marriage/Civil Partner certificate
- Fire brigade ID card
- Non bank savings account
- Mobile telephone contract account
- Buildings insurance
- Contents insurance
- Vehicle insurance
- Home Office Travel Doc
- Fixed the line telephone account
- Gas supply account
- Electricity supply account
- P45
- Financial Statement
- Benefit Statement
- Mortgage Statement
- P60
- Central or Local entitlement document
- Police Bail Sheet
- Letter from Local Authority
- DBS Enhanced Disclosure Certificate
- HMG issued convention travel document
- HMG issued stateless person document
- HMG issued certificate of travel
- HMG issued certificate of identity

ANNEX 2 – SERVICE LEVELS AND SERVICE CREDITS

1. Scope

This Annex 2 sets out the Service Levels which the Contractor is required to achieve when delivering the Services, the Service Credits which the Contractor is required to pay for failing to meet a Required Service Level, the Notification Thresholds, Termination Thresholds and the method by which the Contractor's performance of the Services will be monitored. This Annex comprises:

1.1 Part A: Service Levels and Service Credits;

1.2 Appendix 1 to Part A - Service Levels Detailed Descriptions;

1.3 Appendix 2 to Part A - Summary of Service Levels and Service Credits; and

1.4 Part B: Performance Monitoring.

PART A

1. Principles

1.1 The objectives of the Service Levels and Service Credits are to:

1.1.1 ensure that the Services are of a consistently high quality and meet the requirements of the Authority;

1.1.2 provide a mechanism whereby the Authority can attain meaningful recognition of inconvenience and/or loss resulting from the Contractor's failure to deliver the level of Service which it has contracted to deliver; and

1.1.3 incentivise the Contractor to meet the Service Levels and to remedy any failure to meet the Service Levels expeditiously.

2. Service Levels

2.1 The Service Levels applicable to this Agreement and their corresponding Service Credits are set out in detail in Appendix 1 and Appendix 2 to this Part A.

2.2 The Contractor shall monitor its performance of each of the Services against the Service Level(s) for that Service as set out in Paragraph 2.1 and shall send the Authority a report detailing the level of service which was achieved in accordance with the provisions of Part B of this Annex 2.

2.3 The Contractor shall, at all times, provide the Services in such a manner that the Required Service Level for each Service is achieved.

3. Repeat and Persistent Failures

3.1 If the Contractor fails to achieve the same Required Service Level during six (6) consecutive months or during six (6) months in any twelve (12) months, such failure shall be deemed to be a "**Repeat Failure**".

3.2 In the event of a Repeat Failure, the Contractor shall:

3.2.1 be deemed to have reached the Notification Threshold; and

3.2.2 take all reasonable steps to resolve the underlying cause of the Repeat Failure and prevent recurrence.

3.3 The Contractor shall be deemed to have reached the Termination Threshold in the event of two (2) Repeat Failures.

4. Service Credits

4.1 Service Credits will accrue as set out in Appendix 2 to Part A of this Annex 2 (Service Levels and Service Credits).

4.2 The liability of the Contractor in respect of Service Credits will be limited in accordance with Clause 55.2.5 (Limitations on Liability) of the Framework Agreement.

4.3 The Contractor shall within ten (10) Working Days after the end of the relevant Measurement Period issue a credit note to the Authority for a sum equal to the Service Credits payable for that Measurement Period and such sum shall be recoverable by the Authority in accordance with the relevant provisions of Annex 6 (Charges and Invoicing).

4.4 The Authority shall use the performance reports provided pursuant to Part B of this Annex to, among other things, verify the calculation and accuracy of the Service Credits, if any, applicable to each relevant month.

4.5 Service Credits are a reduction of the amounts payable to the Contractor in respect of the Services and do not include VAT.

5. Nature of Service Credits

The Contractor confirms that it has modelled the Service Credits and has taken them into account both in setting the level of the Charges and in calculating its Financial Model. Both Parties agree that the Service Credits are a reasonable method of price adjustment to reflect poor performance. The Parties acknowledge that the Service Credits represent a genuine pre-estimate of the Authority's direct losses for the Service Failures to which they relate.

6. Application of Thresholds

6.1 If the level of performance of the Contractor of any element of a Service during the relevant Measurement Period:

6.1.1 achieves the Required Service Level in respect of each element of the Service, no Service Credits will accrue in respect of the Services;

6.1.2 is below the Required Service Level but above the Termination Threshold in respect of any element of the Service, the appropriate value of Service Credits shall be payable in respect of that element of the Service;

6.1.3 is below the Notification Threshold in respect of any element of the Service, the Contractor shall undertake the remedial action set out in Clause 11.3 of the Framework Agreement in addition to accruing the Service Credits which are payable in respect of that element of the Service;

6.1.4 constitutes a Critical Service Failure, the Authority shall be entitled to terminate the Agreement pursuant to Clause 58.3.5 (g) (Termination Rights) of the Framework Agreement and/or seek damages at large in addition to accruing the Service Credits which are already payable by the Contractor to the Authority.

6.2 For the avoidance of doubt, any Service Credits paid by the Contractor to the Authority in respect of any Critical Service Failure in accordance with Paragraph 6.1.4 above shall be

deducted from any amount of damages at large sought by the Authority in respect of such Critical Service Failure under Paragraph 6.1.4.

APPENDIX 1 TO PART A

Service Levels Detailed Descriptions

Uptime

The platform used to request and retrieve the results of identity checks will have at least a 99.5% uptime. Uptime is measured on a calendar month basis, is expressed as a percentage and is calculated as follows:

- (actual uptime in minutes in the relevant calendar month / total number of minutes in the relevant calendar month (less Permitted Downtime)) x 100.
- With minutes expressed to two decimal places, rounding up.

("**Uptime**")

"**Permitted Downtime**" is the period of any downtime measured in minutes arising from one of the following events. Permitted Downtime shall not be taken into account when calculating the denominator in the above equation:

- planned maintenance for which Contractor (by itself or through Yoti) has given at least five Working Days' notice (provided that the planned maintenance is limited to 30 hours per calendar month);
- Emergency maintenance to prevent, or in response to, a Priority 1 or Priority 2 issue (as described below);
- Force Majeure Event; or
- Act or omission outside of the control of the Contractor or any Sub-Contractor and for which the Contractor or relevant Sub-contractor is not responsible for under this Call Off Agreement

Response and resolution times for Platform issues

In the event that the Authority experiences downtime that is the fault of the Contractor, the Authority will be able to check status.yoti.com to check if the Contractor is aware of the issue.

- If the issue is listed on status.yoti.com then the Contractor shall resolve the issue within the resolution times below (subject to the note below).
- If the issue is not listed on status.yoti.com then the Authority will be able to contact partnerhelp@yoti.com, who will respond to an email support request from the Authority within the tabulated 'response time' depending on the priority level of the issue. The Contractor reserves the right to re-classify the priority level if it disagrees with the Authority's initial classification and the Contractors decision is final.

Please note:

- 'Response' shall mean the Contractor has confirmed to the Client that the incident has been logged or escalated.
- If due to the complexity of the issue the Contractor considers (acting reasonably) that the incident cannot be resolved within the relevant resolution time below, the Contractor shall promptly notify the Authority and if necessary the parties shall agree a different resolution time for that incident.

Issue Severity	**Response Time (24/7)**	**Resolution Time (24/7)**

Priority 1: ● Complete outage ● Loss or corruption of attribute data in the platform	20 minutes	2 hours
Priority 2: ● Significant impairment to any functionality that is caused by an issue with the Platform	30 minutes	4 hours
Priority 3: ● Platform is operational but with materially reduced functionality. ● Degradation to service performance ● Impairment to service functionality	1 hour	8 hours
Priority 4 ● Minor degradation to service performance	One Working Day	Up to five Working Days

Change Management SLA exclusion

It must be noted that no service development can be deployed during a six week window in November and December due to a Christmas change freeze period. This is the peak time of the year for our branches and hence to enable effective operations we cease all change in the network to enable our postmasters to focus on customer service and not on service changes or training.

Contact Details:
Clients may email partnerhelp@yoti.com

Service Credits
If Uptime falls below the specified level for any month, a Service Credit shall be applied against fees and payments due for the relevant month during which Uptime was not met. This shall be, as liquidated damages and not as a penalty, an amount equal to 3 percent of the fees payable under this Agreement for those months. The credit note raised for this Service Credit shall be applied to the next invoice sent and shall not be available as a refund except where no subsequent invoice is issued, in which case it will be sent as a refund by bank transfer within 30 days of termination of the Agreement.

APPENDIX 2 TO PART A

Summary of Service Levels and Service Credits

Ref.	Service Area	Service Level Description	Measurement Period	Reporting Period	Required Service Level	Notification Threshold	Termination Threshold	Service Credit
1.	Platform	Platform availability other than during planned downtime	Monthly	Monthly	99.5%	As defined in Paragraph 3 of Part A above	As defined in Paragraph 3 of Part A above	Where service level is not met for any measurement period, 3% of the fees payable for the applicable month shall be due as a credit note applied
2.	P1 Incidents	Response to P1 Incidents	Monthly	Monthly	Within 20 minutes	As defined in Paragraph 3 of Part A above	As defined in Paragraph 3 of Part A above	Not applicable
3.	P2 Incidents	Response to P2 Incidents	Monthly	Monthly	Within 30 minutes	As defined in Paragraph 3 of Part A above	As defined in Paragraph 3 of Part A above	Not applicable
4.	P3 Incidents	Response to P3 Incidents	Monthly	Monthly	Within one hour	As defined in Paragraph 3 of Part A above	As defined in Paragraph 3 of Part A above	Not applicable
5.	P1 Incidents	Resolution of P1 Incidents	Monthly	Monthly	Within 2 hours*	As defined in Paragraph 3 of Part A above	As defined in Paragraph 3 of Part A above	Not applicable
6.	P2 Incidents	Resolution of P2 Incidents	Monthly	Monthly	Within 4 hours*	As defined in Paragraph 3	As defined in Paragraph 3	Not applicable

						of Part A above	of Part A above	
7.	P3 Incidents	Resolution of P3 Incidents	Monthly	Monthly	Within 8 hours*	As defined in Paragraph 3 of Part A above	As defined in Paragraph 3 of Part A above	Not applicable

* Or different resolution times for particular incidents agreed pursuant to the "Please note" section in Appendix 1 to Part A above.

PART B

Performance Monitoring

This Part B is to be read in conjunction with Schedule 8.1 (Governance) of the Framework Agreement.

1. Principles

1.1 This Part B provides the methodology for monitoring the Services:

1.1.1 to ensure that the Contractor is complying with the Service Levels; and

1.1.2 for identifying any Service Failures in the performance of the Contractor and/or delivery of the Services ("**Performance Monitoring System**").

1.2 Within twenty (20) Working Days of the Effective Date the Contractor shall provide the Authority with a Performance Monitoring System for the Authority's approval (not to be unreasonably withheld or delayed) which shall, as a minimum, include details of the Contractor's proposals in respect of the following:

1.2.1 performance review;

1.2 Authority audit;

1.2.3 the processes and systems the Contractor will put in place to monitor effectively its performance of the Services as against the Service Levels;

1.2.4 the format and content of the Performance Monitoring Report; and

1.2.5 how the Contractor will comply with the obligations set out in Part B of this Annex 2.

1.3 The Authority shall notify the Contractor within ten (10) Working Days of its receipt of the draft Performance Monitoring System of its response (approval or rejection) to it. The draft Performance Monitoring System shall not be deemed to have been approved if no notice of approval is given during such period. If the draft Performance Monitoring System is approved by the Authority it shall be adopted immediately.

1.4 If the Authority gives notice of its rejection of the draft Performance Monitoring System, it shall in such notice identify the changes it requires to be made to it. The Contractor shall amend the draft Performance Monitoring System so as to incorporate the changes required by the Authority and re-submit the amended draft Performance Monitoring System to the Authority for approval within five (5) Working Days of receipt of the Authority's rejection notice. If the Authority does not approve the draft Performance Monitoring System following its resubmission to the Authority pursuant to the provisions of this Paragraph 1.4, the matter shall be resolved in accordance with the Dispute Resolution Procedure.

1.5 The Contractor shall ensure that the Performance Monitoring System shall be maintained and updated by the Contractor as may be necessary to reflect the then current state of the Services. An updated Performance Monitoring System shall be forwarded to the Authority for approval at least once every month during the Term in accordance with the agreed reporting schedule, and within five (5) Working Days of receipt by the Contractor of any request from the Authority for an update. The Authority shall be entitled to require reasonable amendments to the updated Performance Monitoring System and the Contractor shall make such amendments and re-submit a further updated Performance Monitoring System to the Authority for approval. Until such time as the updated Performance Monitoring System is approved by the Authority the Performance Monitoring System then existing (that is to say prior to the update) shall continue to apply.

1.6 The Parties shall consider and review the Performance Monitoring System at the Call Off Performance Management Board pursuant to Schedule 8.1 (Governance) of the Framework Agreement.

1.7 The Authority shall be entitled to reasonably require changes to the Performance Monitoring System, which shall be implemented in accordance with the Change Control Procedure.

1.8 Without prejudice to the provisions of Paragraphs 1.5 and 1.7 of this Part B each of the Authority and the Contractor shall have the right to propose any Changes to the Performance Monitoring System in accordance with the Change Control Procedure. For the avoidance of doubt, any requests for Changes to the Performance Monitoring System shall be dealt with via the Change Control Procedure.

2. Performance Monitoring and Performance Review

2.1 Within ten (10) Working Days of the end of each month, the Contractor shall provide a Performance Monitoring Report to the Authority.

2.2 The Performance Monitoring Report shall be in the format set out in the Performance Monitoring System and shall contain, as a minimum, the following information in respect of the month just ended:

2.2.1 the monitoring which has been performed in accordance with the Performance Monitoring System with a summary of any issues identified by such monitoring including any occurrences of the Service Failures having the effect of taking the Service Levels below the Notification Thresholds;

2.2.2 for each Service Level, the actual performance achieved over the month, and that achieved over the previous three (3) months;

2.2.3 a summary of all Service Failures that occurred during the Measurement Period;

2.2.4 the level of each Service Failure which occurred;

2.2.5 which Service Failures remain outstanding and progress in resolving them, the cause of the fault and any action being taken to reduce the likelihood of recurrence;

2.2.6 for any Repeat Failures, actions taken to resolve the underlying cause and prevent recurrence;

2.2.7 the Service Credits to be applied in respect of that month indicating the Service Failure(s) to which the Service Credits relate;

2.2.8 a rolling total of the number of Service Failures that have occurred and the amount of Service Credits that have been incurred by the Contractor over the past six (6) months;

2.2.9 relevant particulars of any aspects of the performance by the Contractor which fail to meet the requirements of the Agreement; and

2.2.10 such other details as the Authority may reasonably require from time to time.

2.3 The draft Performance Monitoring Report shall be reviewed and its contents agreed by the Parties at the Performance Review Meeting which immediately follows the issue of such report in accordance with Paragraph 2.5 of this Part B.

2.4 The Contractor shall provide the Authority with a quarterly written summary of the Performance Monitoring Reports that have been prepared during that Quarter ("**Quarterly Summary**"). The Quarterly Summary shall be provided by the Contractor to the Authority within five (5) Working Days of the end of each Quarter, and shall be reviewed at the Performance Review Meeting which immediately follows its issue. The Quarterly Summary shall contain such details as the Authority shall reasonably require.

2.5 The Parties shall attend Performance Review Meetings on a monthly basis (unless otherwise agreed). The Performance Review Meetings will be the forum for the review by the Contractor and the Authority of the Performance Monitoring Reports and Quarterly Summaries (where relevant). The Performance Review Meetings shall (unless otherwise agreed):

2.5.1 take place within one (1) week of the Performance Monitoring Report being issued by the Contractor;

2.5.2 take place at such location and time (within normal business hours) as the Authority shall reasonably require unless otherwise agreed in advance;

2.5.3 be attended by the Contractor and the Authority; and

2.5.4 be fully minuted by the Contractor. The Contractor shall provide to the Authority the prepared minutes within two (2) Working Days from the date of the relevant meeting for its approval and, once approved, the Contractor shall circulate the approved minutes to all other attendees at the relevant meeting and to any other recipients agreed at the relevant meeting.

2.6 The Authority shall be entitled to raise any additional questions and/or request any further information regarding any Service Failure.

2.7 The Contractor shall provide to the Authority such supporting documentation as the Authority may reasonably require in order to verify the level of the performance by the Contractor and the calculations of the amount of Service Credits for any specified period.

3. Satisfaction Surveys

3.1 In order to assess the level of performance of the Contractor, the Authority may undertake satisfaction surveys in respect of Customers or various groups of Customers ("**Satisfaction Surveys**"). These surveys may consider:

3.1.1 the assessment of the Contractor's performance by Customers against the agreed Service Levels; and/or

3.1.2 other suggestions for improvements to the Services.

3.2 The Authority shall be entitled to notify the Contractor of any aspects of their performance of the Services which the responses to the Satisfaction Surveys reasonably suggest are not meeting the Authority Requirements.

3.3 The Contractor shall, as soon as reasonably practicable after notification from the Authority in accordance with Paragraph 3.2 of this Part B ensure that such measures are taken by it as are appropriate to achieve such improvements as soon as is reasonably practicable.

3.4 All other suggestions for improvements to the Services shall be dealt with as part of the continuous improvement programme pursuant to Schedule 2.4 (Continuous Improvement) of the Framework Agreement.

4. Records

4.1 The Contractor shall keep appropriate documents and records (e.g. Help Desk records, Service Failure log, staff records, timesheets, training programmes, staff training records, goods received documentation, supplier accreditation records, complaints received etc) in relation to the Services being delivered and the other requirements to be satisfied. Without prejudice to the generality of the foregoing, the Contractor shall maintain accurate records of call histories for a minimum of twelve (12) months and provide prompt access to such records to the Authority upon the Authority's request. The records and documents of the Contractor shall be available for inspection by the Authority and/or its nominee at any time and the Authority and/or its nominee may make copies of any such records and documents.

4.1.1 In addition to the requirement in Paragraph 4.1 of this Part B to maintain appropriate documents and records, the Contractor shall provide to the Authority such supporting documentation as the Authority may reasonably require in order to verify the level of the performance of the Contractor both before and after the Cut Over Date and the calculations of the amount of Service Credits for any specified period.

4.1.2 The Contractor shall ensure that the Performance Monitoring System and any variations or amendments thereto, the Performance Monitoring Report, any reports and summaries

produced in accordance with this Annex and any other document or record reasonably required by the Authority are available to the Authority on-line and capable of being printed.

ANNEX 3 – CONTRACTOR SOLUTION

Introduction

Post Office is delighted to submit this response to GDS' tender for a face-to-face channel to support the GOV.UK One Login programme. Post Office has decades of experience delivering identity services through its branch network for both the public and private sector and has worked on previous government identity services such as the GOV.UK Verify scheme and in person identity verification for the Disclosure and Barring Service. Providing inclusive services is part of our social purpose and we are continually looking at how we can expand and extend our reach to further accommodate broader populations of citizens.

In order to provide the face-to-face service prescribed by this contract, Post Office will appoint Yoti as a subcontractor. Post Office and Yoti have an existing business relationship providing identity services to the UK, and which underpins the in-branch verification (IBV) service which we are offering to GDS in this tender.

In-Branch Verification is a service for organisations who require In-person identity verification and document validation with the convenience of Post Office's Identity Service branches. The service combines the strengths of Yoti's advanced digital identity verification and document validation capabilities with the convenience and accessibility and experience of Post Office postmasters in our growing network of enabled branches across the UK.

We launched our new IBV service in April 2022, it was delivered following an extensive design and due diligence exercise with an ambition to modernise the legacy service, maintaining our excellence in customer service whilst enabling the leverage of back-office identity verification technologies and greater alignment with achievement of GPG44/45 standards.

Yoti has been in the market since its incorporation in 2014. Having built on its intention to deliver privacy-preserving, secure identity solutions to the consumer marketplace, its product offerings have matured in line with both market forces and technological innovations over the intervening years. Now Yoti has a full suite of services both B2C and B2B to offer to its established and growing client base. Full maturity of the product offering has most recently culminated with the delivery of the in-branch verification service in partnership with Post Office.

This bid is submitted in line with the RM3707 Front Office Counters (FOCs) Framework terms and conditions.

The Service

The service utilised in this proposal is the Post Office in-branch verification service (IBV), built in partnership with Yoti, and facilitated through the Post Office branch network. As Post Office's subcontractor, Yoti will deliver 80% of the service.

In-Branch Verification is a service for organisations who require In-person identity verification and document validation with the convenience of Post Office's Identity Service branches. The service combines the strengths of Yoti's advanced digital identity verification and document validation capabilities with the convenience and accessibility and experience of Post Office postmasters in our growing network of enabled branches across the UK.

The service is ideal for organisations who require additional assurance to meet business risk or regulatory obligations, or where customers require the additional assistance that a Post Office branch can provide.

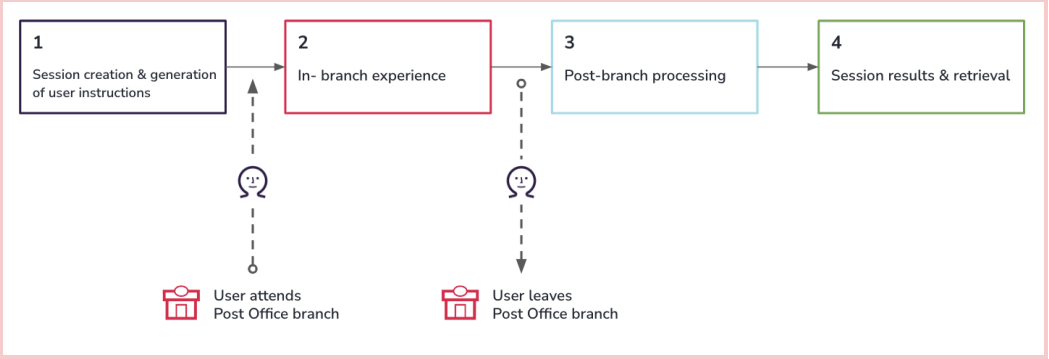
For organisations: "From basic document checking to highly assured digital identity verification, Post Office can help you establish trust with customers, employees or partners in our UK wide service."

For customers: "You keep your original documents, and we send digital verified copies to the person or company who has requested the checks."

In this response we have broken the service down into four core components:

1. Session creation and generation of user instructions
2. In-branch experience

3. Post branch processing
4. Session results and retrieval



For each of the elements there follows a summary of the processes which are to be performed as part of the overall service.

(1) Session creation, generation of user instructions

- The session is initiated from the citizen interaction with the GDS One Login service.
- The citizen is passed to the service to make decisions around branch locations and document types that they will take with them.
- This is formalised in a letter or digital attachment for them to take with them, with a clear set of instructions.

(2) In branch experience

- Once in branch, the postmaster utilises the unique transaction identifier (QR code) to retrieve instructions. The postmaster will perform a “fast-fail” check to make sure the citizen has the correct documents to perform the check.
- The postmaster will then complete the document scanning and facial image capture and review before submitting back to the service.
- Postmasters are trained specifically in how to execute the IBV service. Additionally, within the service app there is a ‘training mode’ so that they can perform refresher training utilising the actual service. Within the app there are screen prompts and help text throughout the journey.

(3) Post branch processing

Once the session has been facilitated in the branch, the information is passed through the service to the Yoti backend, where the post processing takes place in both an automated and manual process (where required) within the Yoti admin system, within the London-based security review centre.

These checks use the same technology and operational elements as the identity service certified under the UK Digital Identity & Attributes Trust Framework.

Yoti UK Security Centre processing

- Visual document authenticity & comparison to template
- Face match (fallback from automated)
- Manual text extracted (fallback from automated)

Yoti backend automated processing

- OCR data extraction
- Automated face matching
- Cryptographic validation of NFC chip payload
- MRZ format validation
- UK DL number validation

Face matching

- Combined with 'liveness' (proven by the citizen in attending the Post Office branch), this face match achieves verification score '3' under GPG45.
- We use a NIST FRVT-listed face matching provider, hosted on-premise.
- Current algorithm performs with 99.8% True Match Rate at a False Match Rate of 10^{-6}
- The service does not recommend a face match check is rejected based on the outcome of automated matching alone. An automated face match check failure will fall back to a manual 'super recogniser'.

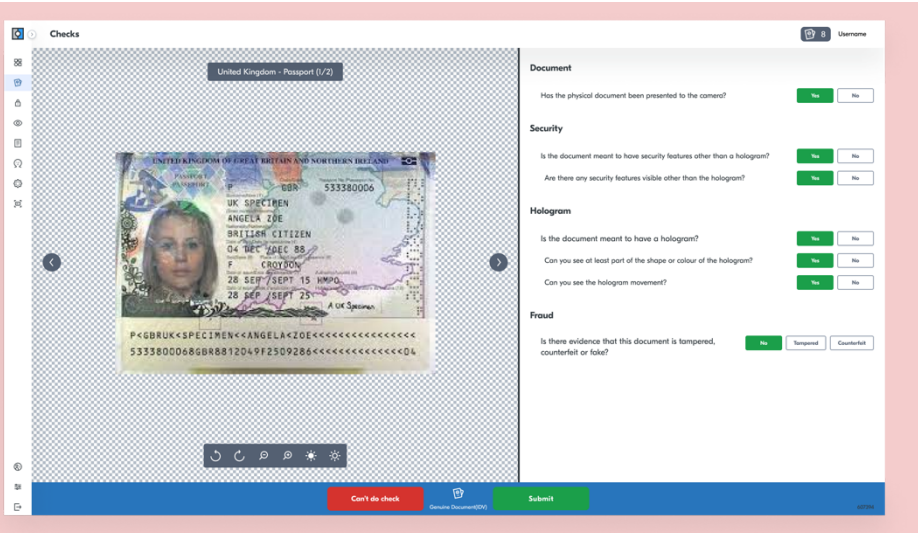
NFC Chip validation

- The service will extract data from the MRZ and the embedded chip, including a digital copy of the same face photo as printed on the document photo page
- The chip payload is validated, as well as checking that the Security Object Document is present
- The service verifies the digital signature and trust chain, and checks that the Country Signing Certification Authority (CSCA) Certificate is trusted
- This face photo extracted from the chip (this 'chip' face photo is used for the face match check)

Yoti Admin System

Yoti has designed, built, deployed, and constantly iterates its internal review system. This system allows for the visual checking of documents and other elements as the result of the "manual fallback" process. The system is delivered in a secure environment, with the access control restricted to the staff whose role it is to work within the security centre. As a note the provision of the access control, CCTV, and other security systems within the Yoti real estate is provided by an NSI accredited provider. The terminals that the admin system run on are highly restricted with no external access to the wider internet, they also have functionality such as screen captures, and external device access blocked. No electronic devices are allowed into the security centre and all staff are supervised whilst within it.

From the images below you can see that the document reviewers are guided through the checking process.



Yoti has deployed the most current versions of Keesing's document validation repository alongside access to PRADO, these are update as they become available. In addition to this, Yoti maintains an internal wiki which is built upon intelligence and experience of document handling from all our security centres and information gathered as part of our research function.

Yoti's security centre employs specialist super recognisers who operate the back-office service. Candidates are recruited through a three step process which takes 4 weeks:

- Stage 1: Facial recognition tests and data/document verification
- Stage 2: Online testing for facial recognition & on site data entry testing
- Stage 3: Onsite competency-based interview and final facial recognition tests

Pre-Employment Checks are carried out as follows:

- Identity / Right to work check, Employment references, Disclosure & Barring Service basic criminal records check, TransUnion check (validates bank details and provides fraud warnings if they are linked to a different bank account. Flags court and insolvency data e.g. County Court Judgements (CCJs), Voluntary Arrangements and Bankruptcies, checks electoral roll information, linked addresses), CIFAS internal fraud database check

Once recruited employees go through a 7 week training schedule. The checker is on probation for 6 months, during which a minimum of 10% of their checks are reviewed daily.
Once probation is completed, and their accuracy rate is above 98%, then 2% of their volumes per day are checked.

(4) Session results and retrieval

By utilising a webhook you can get updates as to the status of the session. After collection, submission and processing of the identity information is completed, you will be notified by the defined webhook and can collect the generated report as well as calling-back the session media. Within this mechanism there is the ability to delete the information once received or allow a system settings to deal with the deletion upon reaching the set timeframe. It should be noted that information reviewed in the admin system remains available to the subcontractor's London security centre for a period of 28-days.

Report Structure

- Primary report contains no PII but lists outcomes of all checks performed and links to "resources" and "media".
- Each check is given an overall recommendation, and most checks contain sub-checks for inspection.
- Data extracted from documents is available within the document resource object.

Data retention

- Once retrieved, GDS can delete all data associated with a session, or delete specific media associated with a session (leaving the report which does not contain PII).
- Data not deleted explicitly will be removed when the 'time to live', set by GDS at session creation time, expires.
- All data associated with the GDS IBV session will be stored with our UK datacentres and an AWS S3 bucket in AWS London Datacentre.

Check recommendations (outcomes)

When the outcomes are provided back from the service, there are two types of responses for failure, noted in the below table are the reasons associated with each.

Recommendation 'not available'	*Recommendation 'reject'*
Expected to happen very rarely due to Postmaster training. Indicates that security centre staff could not perform the check due to a problem with the submitted document / images. Retry action generally recommended. **Reasons such as:** • Glare (obstruction) in image • Document too damaged • Photo too blurry / dark	Indicates that there is a reason to reject this check. **Reasons such as:** • NFC chip validation failed • Suspected counterfeit / tampered • Face does not match between ID document and face photo • Document number invalid

Fraud management: In-branch

- Where suspicious activity is suspected by a postmaster during a branch check, then the postmaster will complete the transaction without tipping-off the customer. Documents will be digitised and provided to the Yoti Security Centre for expert assessment.
- Postmasters will raise a suspicious activity report using Post Office internal fraud reporting tool (Grapevine). Reports to Grapevine are typically made by Postmasters or branch employees immediately following a suspicious activity or on the same Working Day following an incident in branch. Where a client is named (ie. One Login), the Post Office Security team will (using their best endeavours) provide a copy of relevant details to the client as soon as possible (and whenever practicable no later than the end of normal business hours on the next Working Day following the relevant event), to enable further gathering of relevant information from the postmaster, branch and client. If 'Gov.UK One Login' is not named in the Suspicious Activity Report, we are unable to provide notification to the Authority.
- Reasons for suspicious activity include:
    - External prompting - during the transaction the customer received prompting from others indicating that they may be undertaking the transaction under duress.
    - Suspicious behaviour - the way a customer behaves, or comments made are outside the range that a postmaster would reasonably expect for this type of transaction, creating concern or suspicion about the customer.
    - Suspicious document - where a document appears to have been tampered with or is suspected as counterfeit.
    - Disguise - where heavy make-up or facial prosthetics may be being used by the customer to attempt to disguise their true facial features.

Fraud management: Post branch processing

- Where fraud is detected or suspected during post-branch checks, the associated check will be returned to GDS with a recommendation 'reject' and the relevant reason. In this way fraud information is always available to GDS at a granular level.
- All security centre staff are trained in fraud detection for document validation and face matching. Face matching is only completed by super recognisers.
- Yoti also employs a dedicated counter-fraud team, who have access to a dedicated area within our secure web-app to investigate cases of suspected or detected fraud (for up to 28 days after the check was submitted). All staff delivering the service are geographically located in the UK. To meet the Authority requirements for UK-only data processing, access to Authority Data has been restricted to UK-only personnel. This control applies to all current and future personnel.

Incorrect documents presented in-branch

- Where a citizen presents documents in branch that do not match those specified at the time of session creation, then the postmaster will advise the customer of the error and that they can return with the correct documents at a later stage.
- Should the customer not have the documents they initially claimed to have, they will be advised to contact the requesting client (GOV.UK One Login) so that a new IBV session can be created.
- Document substitutions are not accepted or supported by the service.

Documents supported (MVP/V1)

	GPG45 strength score	GPG45 validation score	Notes
UK Passport	4	3 (or 2 if NFC read unsuccessful)	Automated processing: OCR data extraction and validation, NFC DG validation, biometric face matching. UK Security Centre processing: visual authenticity validation against reference templates where NFC is unavailable, visual face match where low-confidence automated result.
Non-UK Passport	4 or 3	3 (or 2 if NFC read unsuccessful)	
UK Driving Licence	3	2	Automated processing: OCR data extraction and validation, biometric face matching. UK Security Centre processing: visual authenticity validation against reference templates, visual face match where low-confidence automated result.
UK Biometric Residence Permit	4	2	
EU Driving Licence	3	2	
EU National ID Card	3	2	
Citizencard & Post Office PASS card	3	2 (but issuing authority check adds assurance)	***To follow as soon as agreed, after v1 launch*** Automated processing: OCR data extraction and validation, biometric face matching and issuing authority validation. UK Security Centre processing: visual authenticity validation against reference templates, visual face match where low-confidence automated result.
Young Scot card	3	2	

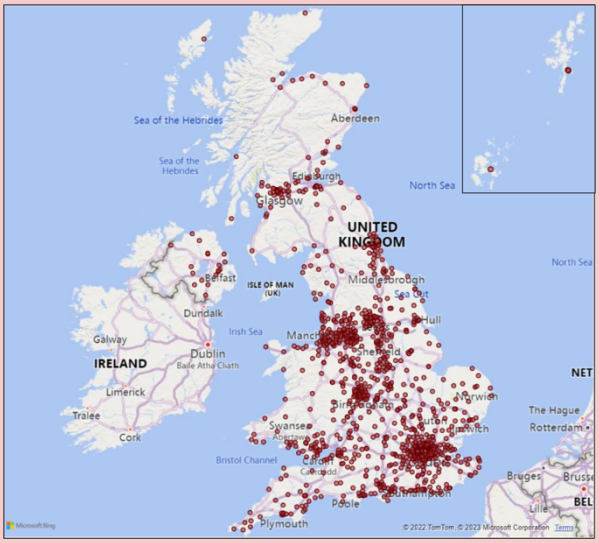
Document checking criteria

Check	GPG45 Score	Criteria	Postmaster	System check	Security Centre
Strength	3	Ascertain UK Driving Licence Photocard is valid and matches individual	Postmaster ensures that document type and issuing country are as specified in the IBV session parameters. Back Office and Security Centre checks confirm the document type, enabling the OneLogin service to determine the applicable document strength score. Document validity and face match verification tasks are detailed in later 'Validation' and 'Verification' sections of this table.	N/A	N/A
Strength	4	Ascertain UK Biometric Passport is valid and matches individual	As above	N/A	N/A
Strength	4	Ascertain Non-UK Biometric Passport is valid and matches individual	As above	N/A	N/A
Strength	4	Ascertain BRP is valid and matches individual	As above	N/A	N/A
Validation	2	Check of physical/printed features of the document	Postmaster is guided to check the following: - Name: First, middle name(s) and surname must all match application exactly and in full. (The name variations are defined per document. I.e., initials vs full names etc) - Date: [document] must be in date and not expired. (Note: default behaviour	OCR data extraction is utilised within the IBV application (client side) to enable the NFC DG's to be accessed.	Where NFC is not extracted, document visual inspection is completed by the Security Centre to obtain a document validation score of 2.

			for IBV is for document to be in-date) The following instructions vary depending on document type - Passport is provided as an example: - Condition: Passport must not be damaged or have any pages or corners removed - Look & feel: Pages and cover should look and feel genuine. - Security features: vignettes, holograms, watermarks, and embossing must all be present		
Validation	3	Checking cryptographically signed features (NFC chip), including: ● read the cryptographically protected information ● provide any required cryptographic keys ● check the evidence has not expired ● check the digital signature is correct ● signing key belongs to the organisation that issued the evidence ● signing key is the correct type for that evidence ● signing key has not been revoked	N/A	Passport NFC issuing authority signature checked enabling document validation score of 3. Where NFC is unable to be extracted, MRZ validation and visual document inspection are completed to provide a document validation score of 2 (see previous row).	N/A
Validation	4	Confirming further security features in person, such as: ● confirm the visible security features are genuine ● confirm the UV or IR security features are genuine	N/A - Validation 4 requires non-visible light spectrum security feature inspection which is not available in branch, hence back office and security centre checks cannot be undertaken.	N/A	N/A

		● confirm the cryptographic security features on the evidence are genuine ● check the evidence has not been cancelled, lost, or stolen ● check the evidence has not expired			
Verification	2	Person based identity verification matching - Ensure the person physically matches the photo on or associated with the strongest piece of genuine evidence you have of the claimed identity (you can do this in person or remotely)	Note: Postmaster does not meet GPG45 requirements: - have been trained in how to detect impostors by a specialist trainer, such as the Home Office, National Document Fraud Unit, CPNI or any other company that follows the Home Office's best practice guidance - refresh their training at least every 3 years	Automated biometric matching is undertaken using a NIST certified component service. Where confidence match rates are insufficient, final determination is made by manual Security Centre assessment.	Facial matching is completed by Security Centre to compare photo ID with customer photo (non-ICAO grade image captured in branch)
Verification	3	Person based identity verification matching - Ensure the person physically matches the photo on or associated with the strongest piece of genuine evidence you have of the claimed identity (you can do this in person or remotely) System based identity verification matching - Ensure the person's biometric information matches biometric information from the strongest piece of genuine evidence you have or an authoritative source	N/A	Automated biometric matching is undertaken using a NIST certified component service. Where confidence match rates are insufficient, final determination is made by manual Security Centre assessment.	Facial matching is completed by Security Centre to compare photo ID with customer photo (non-ICAO grade image captured in branch)

Post Office IBV enabled branch locations



96.8% of the UK population live within 10 miles of a branch offering the IBV service

Devolved Nations reach within 10 miles:

England: 98.4%
Northern Ireland: 79.2%
Scotland: 87.6%
Wales: 94.5%

The current distribution of the IBV service across the Post Office branch network reaches an overall population coverage 96.8% living within 10 miles of an enabled branch. We commit to the Authority's requirement that this must always remain over 85% and are open to discuss network expansion requirements.

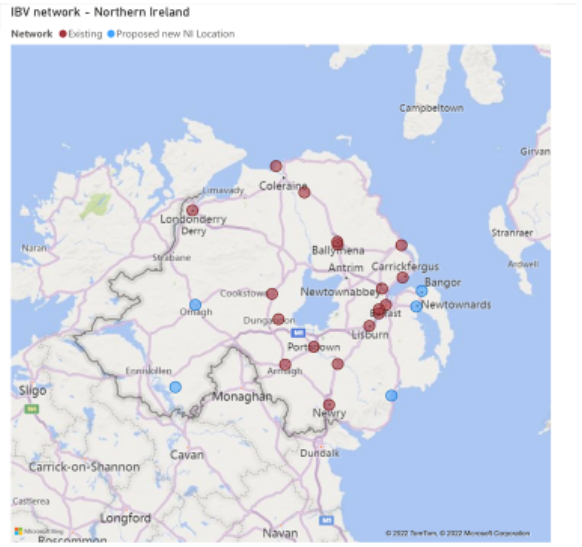
Post Office have planned and costed for an increase of the IBV enabled network in Northern Ireland to increase the accessibility to 86.9% were the Authority to decide that this was needed (see appendix 9 for more information). Please note that if the Authority wants to expand the network then analysis at the time of the request would be re-run and it may be determined that different branches are now more suitable for the expansion due to the ever evolving nature of our network.

Northern Ireland Expansion Proposal

Adding 4 additional branches to the current IBV enabled network:

- Omagh – BT78 1EE
- Newtownards Centre – BT23 4EU
- Donard – BT33 0AL
- Lisnaskea – BT92 0JE

86.9% of the Northern Ireland population would live within 10miles of a branch offering the IBV service.



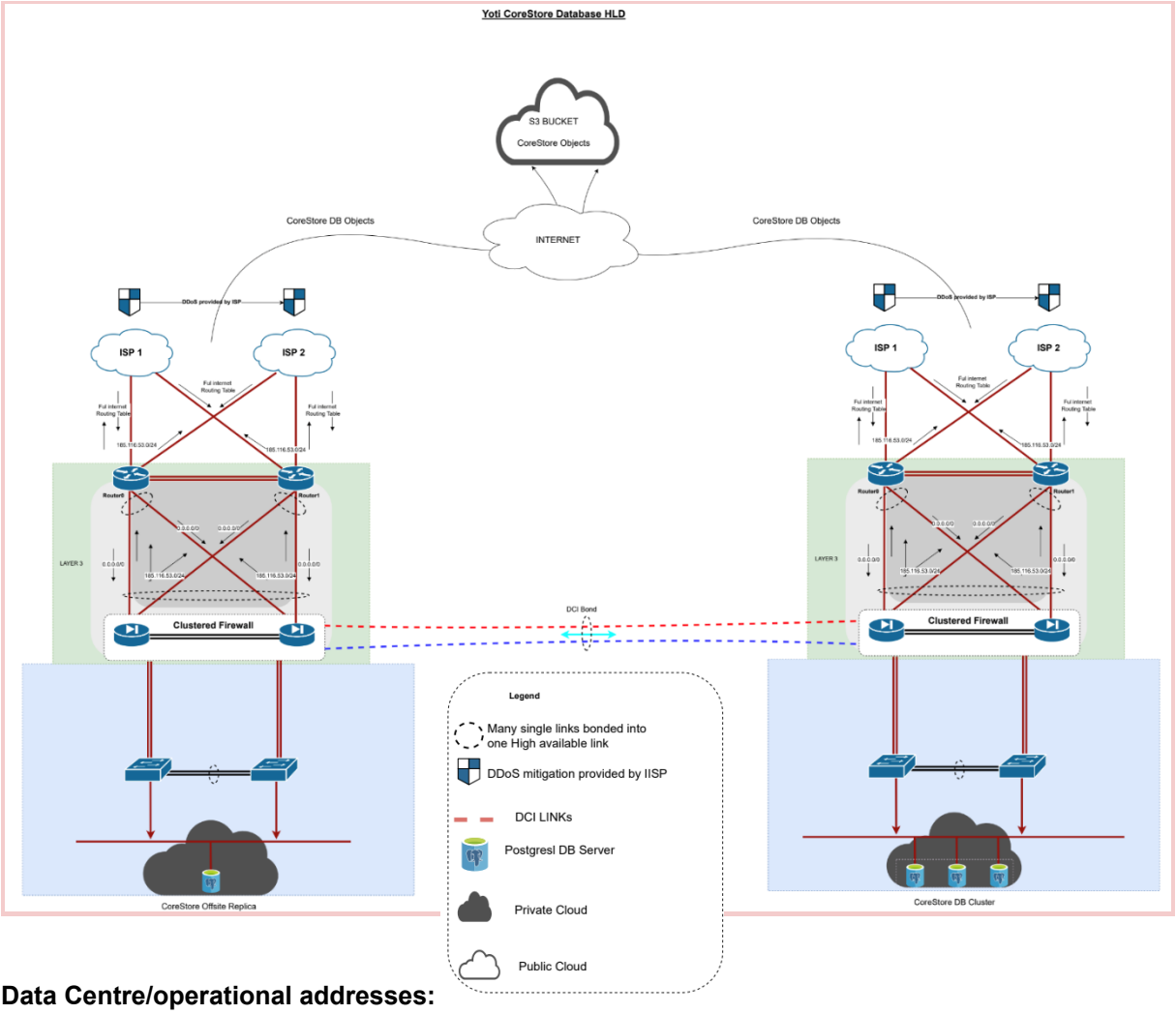
Network expansion of 4 new branches	One-off Cost	Annual Service Management Cost
Expansion Project Cost	£10,000	
Branch Cost (4 branches)	£3,600	£2,400
TOTAL (approx. costs)	**£13,600**	**£2,400 / annum**

If any branch transacts less than 8 transactions per month a fee of £25 will be charged to enable refresher training for staff at that branch to ensure quality of service.

5. Security, data management and compliance

Post Office and the subcontractor are committed to fulfilling the need that all parts of the services associated with the delivery of in-branch verification maintain all data within the UK. All staff delivering the service are geographically located in the UK. To meet the Authority requirements for UK-only data processing, access to Authority Data has been restricted to personnel located in the UK. This control applies to all current and future personnel.

All data for the provision of this service will be routed and stored within our own infrastructure in the Telehouse West and LD5 data centres. The operators of these data centres hold PCI DSS and SOC2 audits for operational security management requirements. In addition to this, we have an encrypted object store in an AWS S3 bucket in AWS London's datacentre. A diagram of this infrastructure arrangement is below.



Data Centre/operational addresses:

Yoti SC: 6th Floor, Bankside House, 107 Leadenhall St, London, EC3A 4AF.
LD5: Slough Trading Estate, 8 Buckingham Ave, Slough, SL1 4AX.
Telehouse West: Coriander Ave, London, E14 2AA.
AWS London: 60 Holborn Viaduct, London, EC1A 2FD.

The subcontractor does allow some team members to work remotely. Those undertaking further development of the service do not have access to any PII from this or any other service and there are significant security controls in place, such as VPNs, MFA, security policies etc. to minimise any risk associated with this hybrid working methodology.

The subcontractor's customer service team will only be allowed access to any GDS PII as part of a triage service if needed, this will be facilitated out of the UK security centre. Whilst this is expected to

be infrequent, the ability to investigate sessions can provide a valuable tool in the monitoring of the service.

Yoti's network operations centre is located within our Bengaluru office in India and is a function that cannot be moved due to its operational impact and 24-hour nature. This team are there to maintain the overall provision and security of the global services deployed by Yoti and have no access to any PII.

Full policies covering data breaches and the management of them has been provided in the subcontractor's incident management policy (appendix 19).

A full review and response to the Security Schedule has been provided in Appendix 1 of Annex 3 (Contractor Solution) which the Parties have reviewed and is in an agreed form.

It is noted that the contractor and sub-contractor must have Cyber Essentials Plus certification, and this is held by Post Office. The certificate has been shared as "Appendix 7".

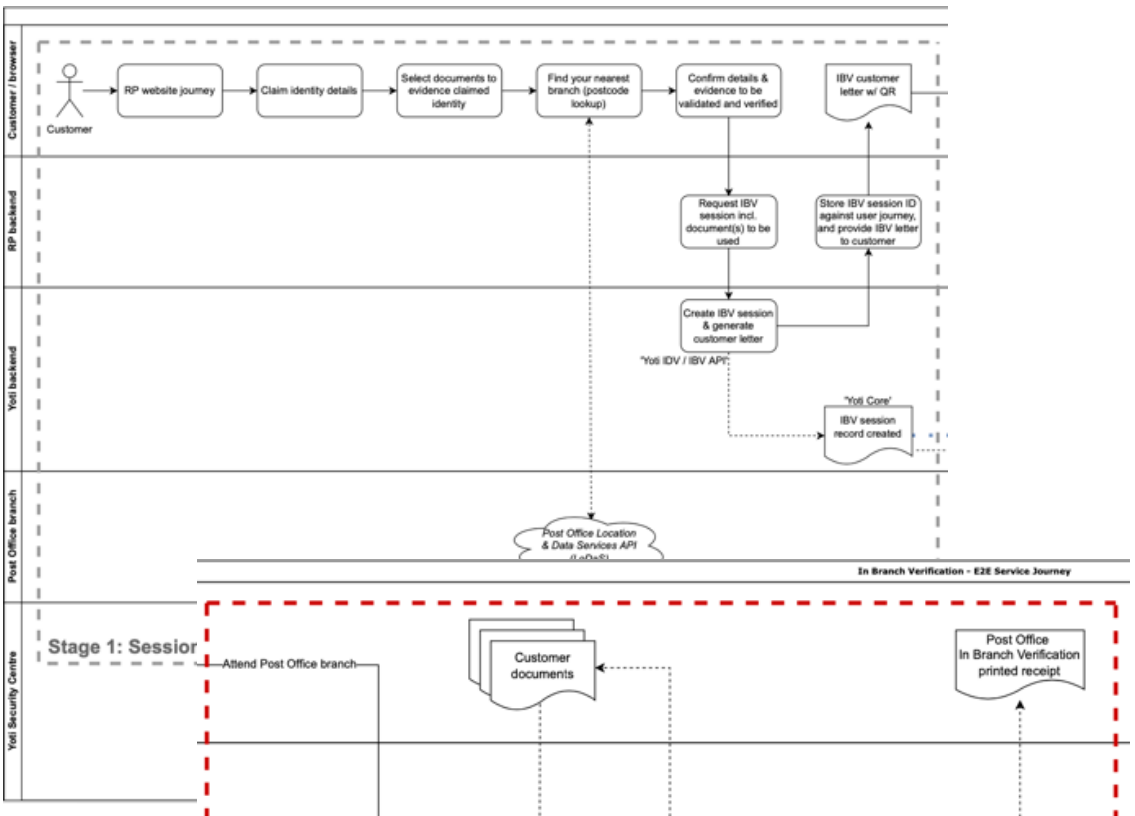
For the subcontractor this is a "not met" requirement within the schedule. The need for the subcontractor, due to being both an SMP and high-risk subcontractor, is to have cyber essential plus certification. Yoti does not maintain this accreditation as its focus has been delivering its services to a global audience, for which it has chosen to implement an ISO27001 certified ISMS and a SOC2 security controls framework. Yoti has previously conducted a compliance review to identify gaps in our certifications when aligned with the requirements of Cyber Essentials Plus.

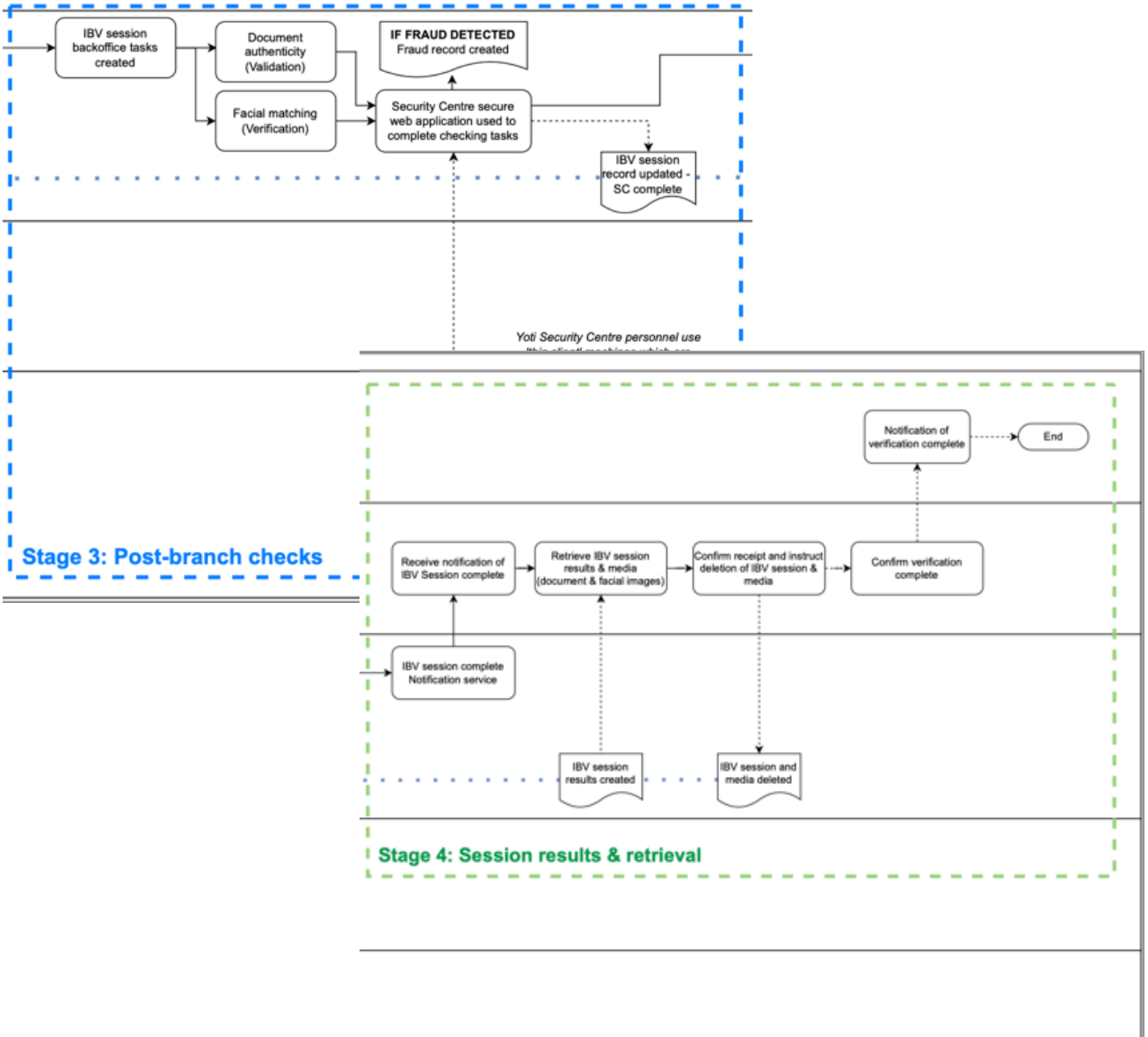
Following this recent review, Yoti has already closed gaps identified such as with BYOD (bring your own device) and staff device policies and is willing within the early term of the contract to progress with the Cyber Essentials Plus audit. However, it should be noted that this action will involve external third parties to be scheduled, the timing of which is out of Yoti's control.

As a closing note on Cyber Essentials Plus, the Yoti platform and services have been designed from the ground up with layered cryptography and rigorous network/environment segregation, which means that end-user data (PII) is never accessible to Yoti staff in unencrypted form on such devices, only within our Security Centres via the above-mentioned terminals, on a secure VPN with no general internet access or ability to run other applications.

Data flows within the service

We have provided Appendix 22: Data Processing & Roles document, along with a diagram as an attachment in Appendix 3: IBV-IDV-Systems&Data-16Jan23 v1.0, which details the overall service provision, staged into the 4 core parts of the process, to demonstrate where the data points are and where the information is captured and distributed to within the Contractor and subcontractor domains.




IBV session backoffice tasks created
Document authenticity (Validation)
Facial matching (Verification)
IF FRAUD DETECTED
Fraud record created
Security Centre secure web application used to complete checking tasks
IBV session record updated - SC complete
Yoti Security Centre personnel use
Stage 3: Post-branch checks
Notification of verification complete
End
Receive notification of IBV Session complete
Retrieve IBV session results & media (document & facial images)
Confirm receipt and instruct deletion of IBV session & media
Confirm verification complete
IBV session complete Notification service
IBV session results created
IBV session and media deleted
Stage 4: Session results & retrieval

Both the Contractor and subcontractor shall comply with the requirements of the Security Schedule.

Asks from GDS for a successful service:

- At least quarterly updates of volume forecasts (to be provided at a per month breakdown) & forthcoming connecting services.
- Transparency of performance - i.e. if there is a sudden unexpected peak of volumes, reasoning to be provided and expectations for future periods.
- Regular sharing of One Login plans to enable service enhancement discussions.
- Feedback on our service received from your customers or RPs.

6. Innovation and continuous improvement

Aligned to Schedule 2.4 (Continuous Improvement) of the Framework Agreement, Post Office and Yoti, collaboratively, shall continually improve the way the Services are delivered throughout the contract term. Planned improvements shall be presented to the Authority during contract review meetings.

Both the Contractor and subcontractor acknowledge the authorities mention of the following improvement areas:

- industry developments.
- changes in relevant standards.
- current and planned Authority policies and guidelines.
- performance and capacity information related to the services.
- information relating to volumetrics, relevant to the Service Requirements including planned and predicted growth rates.
- feedback from Customers on the operational use of the Services and Customer expectations.
- the need to manage and/or mitigate technology risks and service delivery risks.

A foundational level of economic and civic participation is to be able to prove identity. Across our identity services our aim is to enable as many people as possible to have access to identity verification and as such during the contract term, and at key milestones, we will review the following:

- New check types.
- New document types.
- Additional branches.
- Customer feedback and data driven improvements.

The In-Branch Verification (IBV) service was built in partnership with Yoti to provide all the benefits of digital document validation and identity verification to be provided without the need for the customer to interact with a digital device, enabling services and customer journeys to be more inclusive and responsive to individual's needs. Ongoing service improvements are intended to further bridge between physical document checking requirements such as from the Disclosure & Barring Service and GPG45 digital identity verification, including reusable user-centric digital identity services such as Post Office EasyID and Yoti ID.

Upon agreement of any changes and charges, the change notification process will be enacted to deliver service affecting changes.

7. Account, Contract Management and Business Continuity

The key personnel for contractual oversight and management are:

- Elinor Hull - Post Office Identity Services Director (Contract Manager)
- Jason Sheehy - Post Office Product Manager, Identity Services

In addition to the above contract management team, both Post Office and Yoti will leverage colleagues from the following functions to document, implement and continually manage/monitor the service for the duration of the term: Senior Management, Legal, Compliance, infrastructure & security, and product management.

Post Office and Yoti have comprehensive and tested business continuity plans and a provision that covers all of our business operations, which is audited under our cyber essentials plus or SOC2 requirements. We have provided these policies as attachments (annex 14 & 16).

For the provision of reporting for the service, Yoti has a fully integrated BI system (Looker) that can generate standard reports for statistical reports of usage, outcomes, and other key metrics. Yoti will provide standard BI reports on a weekly and monthly basis, covering the previous period.

Ad-hoc reports on the metrics can be provided, the feasibility of these requests will be considered on a case-by-case basis. It is important to convey that Yoti, the subcontractor, does not allow external third-party access to its BI system hence we are unable to provide access to a dashboard for real-time MI.

The following MI/BI shall be provided:

- the volume of applications processed
- the volume of declined applications (citizen)
    - broken down by reason
- geographical location of usage
- utilisation per outlet
- Journeys flagged as suspicious by:
    - type of fraud / document
    - time of fraud
    - location of fraud
    - action taken
- number of outlets available

The following data points are not applicable for the current service:

- a breakdown of outlets by services

the number of rejected applications by Authority

- broken down by reason
- the type of applications
- number and value of any refunds issued

We can confirm that we will provide a detailed contract exit plan and a Business Continuity Recovery Plan within the requested time frame, specific to the service.

8. Social Value

An anchor of UK communities for centuries, Post Office is a commercial business driven by a strong social purpose: to be here, in person, for the people who rely on us. 99.7% of the population lives within 3 miles of one of our 11,500 Post Offices.

We are uniquely placed within every community across the country to help sustain economic recovery, ensuring no-one and no region is left behind. As bank branches close, the Post Office network is seen as critical to small businesses to meet their postal, cash and banking needs. 43% of SMEs say that they would not be able to function without the Post Office.

Post Offices act as a crucial bridge between the online and offline economy. We also help drive footfall to high streets, 400m visits to other high street locations per year are generated by trips to the Post Office, driving an estimated £1.1 billion in additional revenue to the UK economy.

Post Offices are the community hubs of many towns and villages across the UK, especially for older and vulnerable people. For many, Post Office remains an important source of day-to-day social interaction for their wellbeing, while providing access to their essential needs – Post Office is ranked as having the most positive impact in the community by the Association of Convenience Stores.

The Covid-19 pandemic shone a spotlight on the vital lifeline we offer to communities. We worked hard to keep our network open, ensuring that customers, especially the vulnerable, could continue to access our services, even as the high street grew quiet.

A foundational level of economic and civic participation is to be able to prove identity. Since the pandemic, being able to conduct business remotely, in a secure and trusted way, has served to accelerate the need for identity verification. For those that are unable to use smartphones, home computers or afford home internet costs, our in-branch verification (IBV) service supports inclusion, safeguarding of the vulnerable and fraud reduction. Our IBV service is paper free as part of our service design commitment to fighting climate change.

Yoti have supplied their social purpose strategy in Appendix 18: Yoti Social Purpose Strategy.

9. Implementation Plan, Solution Integration and Exit Management Plan

It is proposed that post Effective Date, we will develop a “live” project timeline utilising its Jira implementation for project management. This will allow all contract staff to have visibility of upcoming events and milestones but will not replace the scheduling of contract meetings by traditional methods (Calendar invites/Teams/Google Meets etc.).

In accordance with the Authority’s requirements, we can confirm that a detailed contract exit management plan will be agreed and delivered within 20 Working Days of the Effective Date.

Appendices

The agreed versions of the documents listed below at the Effective Date are contained in the emails sent from Jason Sheehy, Identity Product Manager of the Contractor to:

- (in respect of Appendix 22) Timothy Heads, Commercial Manager of the Authority at 12:02 on 27 June 2023 which the Authority acknowledges was received on that date; and

- (in respect of all other Appendices) Rupinder Aulak, Commercial Manager of the Authority at 16:00 on 21 June 2023 which the Authority acknowledges was received on that date.

Appendix #	Document Title	Description
Appendix 1	Technical Evaluation _ SMS Response – PO-YOTI_GDS 5 _ 6 JUNE2023	Agreed deviations for the purpose of the Contractor's compliance with the Security Schedule
Appendix 2	telehouse-ISO14001.jpg	Yoti Telehouse data centre ISO certificate.
Appendix 3	IBV-IDV-Systems&Data-16Jan23 v1.0.pdf	IDV/IBV data flow diagram.
Appendix 4	Yoti Pen Test Report 2023.pdf	Yoti's latest penetration test.
Appendix 5	Pen test-infrastructure_external_2022_additional_notes.png	Yoti infrastructure and security notes regarding the latest penetration test.
Appendix 6	Penetration findings statement.pdf	Yoti's statement regarding the findings of the latest penetration test.
Appendix 7	Post Office Cyber Essentials Plus Certificate.pdf	Post Office Cyber Essentials Plus Certificate.
Appendix 8	Post Office ISO27001 Certificate (1).PDF	Post Office ISO27001 Certificate.
Appendix 9	IBV Network expansion_301122.pdf	Breakdown of PO IBV expansion proposal.
Appendix 10	Yoti ISO27001 Certification .pdf	Yoti's ISO certificate.
Appendix 11	YT244 Yoti Statement of Applicability v9-0 (2022).pdf	Yoti's ISO 27001 statement of applicability.
Appendix 12	YT064 IT & Infrastructure Security Policy 9-0-1.pdf	Breakdown of Yoti's infrastructure security.
Appendix 13	YT067 Internal - ISMS _ PIMS _ QMS v9.pdf	Yoti's Information Security management System.
Appendix 14	YT113 - Business Continuity Plan v7.0.pdf	Yoti's Business continuity and disaster recovery plan.
Appendix 15	Yoti SOC 2 Type II 2021 vFINAL ELECTRONIC.pdf	Yoti's SOC2 report.

Appendix #	Document Title	Description
Appendix 16	Post Office - Business Continuity Management Policy v2.7	Post Office business continuity and disaster recovery plan.
Appendix 17	POL IT DR Policy V1.4	Post Office disaster recovery policy
Appendix 18	Yoti_Social_Purpose_Strategy	Details of Yoti's social purpose strategy
Appendix 19	YT140 Incident Management Process v6.0.pdf	Yoti's data breach/mitigations/Incident management policies
Appendix 20	Post Office ISO27001-SOA 2021 Final SoA v4.4	Post Office ISO27001 statement of applicability
Appendix 21	equinix-emea-iso-14001-iso-45001-iso-50001-certificate.pdf	Yoti Equinix data centre ISO certificate.
Appendix 22	Data processing and roles - POL_Yoti IBV v2_2.pdf	A breakdown of the data processing flow in its entirety as requested by GDS.

ANNEX 4 – AUTHORITY RESPONSIBILITIES

1. Introduction

1.1 The responsibilities of the Authority set out in this Annex 4 shall constitute the Authority Responsibilities under this Call Off Agreement. Any obligations of the Authority specified in the Annex 1 (Authority Requirements) and Annex 3 (Contractor Solution) shall not be Authority Responsibilities and the Authority shall have no obligation to perform any such obligations unless they are specifically highlighted as "Authority Responsibilities" and cross referenced in the table in Paragraph 3 of this Annex.

1.2 The responsibilities specified within this Annex shall be provided to the Contractor free of charge, unless otherwise agreed between the Parties.

2. General Obligations

2.1 The Authority shall:

2.1.1 perform those obligations which are set out in the Clauses of this Call Off Agreement and the Paragraphs of the Annexes (except Annex 1 (Authority Requirements) and Annex 3 (Contractor Solution) and/or where these are set out under Authority Requirements in this Call Off Agreement);

2.1.2 use its reasonable endeavours to provide the Contractor with access to appropriate members of the Authority's staff, as such access is reasonably requested by the Contractor in order for the Contractor to discharge its obligations throughout the Term;

2.1.3 provide sufficient and suitably qualified staff to fulfil the Authority's roles and duties under this Agreement as defined in the agreed Implementation Plan;

2.1.4 use its reasonable endeavours to provide such documentation, data and/or other information that the Contractor reasonably requests that is necessary to perform its obligations under the terms of this Agreement provided that such documentation, data and/or information is available to the Authority and is authorised for release by the Authority; and

2.1.5 procure for the Contractor such agreed access and use of the Authority's premises, facilities, including relevant ICT systems as is reasonably required for the Contractor to comply with its obligations under this Call Off Agreement, such access to be provided during the Authority's normal normal on each Working Day or otherwise as agreed by the Authority (such agreement not to be unreasonably withheld or delayed).

3. Specific Obligations

The Authority shall, in relation to this Call Off Agreement perform the Authority's responsibilities identified as such in this Call Off Agreement the details of which are set out below:

Document	Location (Paragraph)
Provide the Contractor with at least quarterly updates of volume forecasts (to be provided at a per month breakdown) & forthcoming connecting services.	Data Flows Within the Service Section
Provide the Contractor with reports and updates regarding transparency of performance - i.e. if there is a sudden unexpected peak of volumes. Such reports should include reasoning and expectations for future periods.	Data Flows Within the Service Section
Regular sharing of One Login plans to enable service enhancement discussions.	Data Flows Within the Service Section
Share feedback on the service received from the Users customers or the Authority's representatives.	Data Flows Within the Service Section

ANNEX 5 – OUTLINE IMPLEMENTATION PLAN

None

ANNEX 6 – CHARGES AND INVOICING

PART A - CHARGING

1. Purpose of this Part A of this Annex

The purpose of this Part A of this Annex is to set out the provisions relating to:

1.1 Milestone Payments;

1.2 the Charges applicable to the Services;

1.3 payments for Authority Cause;

1.4 retentions;

1.5 Service Credits;

1.6 Delay Payments;

1.7 Charges for Changes;

1.8 indexation; and

1.9 time and materials Charges.

2. Milestone Payments

2.1 On the issue of the Milestone Achievement Certificate in relation to a Milestone the Contractor will be entitled to deliver an invoice to the Authority in respect of the Charges associated with that Milestone as set out in the table below:

Milestone Number	Milestone Description	Amount of Charge (£)	Reclaimable? [Y/N]
1	Implementation costs 1 (Effective Date)	17,500	Y
2	Implementation costs 2 (service go-live)	17,500	Y
3	Solution integration costs 1 (Effective Date)	70,000	Y
4	Solution integration costs 2 (service go-live)	70,000	Y

The Parties agree that the Contractor may deliver an invoice to the Authority in respect of Milestone 1 and 3 from the Effective Date and that a Milestone Achievement Certificate will not be provided.

2.2 The circumstances in which a Milestone will be considered to have been Achieved are set out in Schedule 6.2 (Testing Procedures). Payment will be made to the Contractor in accordance with Part B of this Annex.

2.3 If any Milestone is not Achieved by its associated Milestone Date then Delay Payments will be applied in accordance with Paragraph 6 of this Annex. If no further Milestone Charges

fall due after Delay Payments accrue, the Contractor shall issue a credit note to the Authority and a sum equal to any such Delay Payments then outstanding shall be repayable by the Contractor to the Authority as a debt.

2.4 The Contractor shall be required to repay to the Authority any reclaimable Milestone Payments under the circumstances set out in Clauses 58.9.2 or 61.6 of the Framework Agreement.

3. Service Charges

3.1 Within thirty (30) days of the end of each Invoicing Period, the Contractor shall deliver an invoice to the Authority (in accordance with Paragraph 2 of Part B to this Annex) in respect of the Service Charges (outlined in Paragraph 3.2 below) for the Services carried out by the Contractor during that Invoicing Period.

3.2 The Authority will pay the Service Charges to the Contractor for all operations services carried out in each Invoicing Period from the Cut Over Date to the end of Term. The Service Charges shall be made up of the following Charges (as applicable):

3.2.1 Fixed Charges in accordance with Paragraph 3.4 below;
less,

3.2.3 any Service Credits payable in accordance with Paragraph 3 of Schedule 2.2 (Service Levels and Service Credits); and/or

3.2.4 any amounts retained or set off by the Authority under Clause 22 (Recovery of Sums Due) of the Framework Agreement.

3.3 The Service Charges will be payable in arrears.

3.4 **Fixed Charges**

3.4.1 The Fixed Charges per transaction to be applied are set out in the table in Appendix 1 to this Annex.

3.4.2 Subject to Paragraph 3.5 below, the aggregate Fixed Charges for each applicable Invoicing Period shall be calculated by multiplying the relevant Fixed Charges per transaction by the relevant number of transactions (regardless of the volume of transactions).

3.5 **Minimum Volume Guarantee**

3.5.1 If following the end of a Quarter the Contractor determines that the volume of transactions for that Quarter is less than the applicable minimum volume guarantee set out in Appendix 1 to this Annex for that Quarter:

(a) the Contractor shall within 10 Working Days of the end of the relevant Quarter provide the Authority with details of its calculation including the Fixed Charges that would have applied for the Quarter if the minimum volume guarantee had been achieved ("**Minimum Fixed Charges**"); and

(b) following approval by the Authority in writing, the Contractor shall be entitled to submit an invoice in accordance with this Call Off Agreement for the difference between the Fixed Charges that were invoiced and the Minimum Fixed Charges.

4. Payments for delays due to Authority Cause

4.1 If the Contractor is entitled to compensation in accordance with Clause 8.5 (Delays to Milestones due to Authority Cause) of the Framework Agreement then such compensation

shall consist of the Contractor's reasonable additional costs arising from such Delay, provided that this calculation shall not operate so as to put the Contractor in a better position than it would have been but for the occurrence of the Authority Cause.

4.2 To the extent that:

4.2.1 any contributory or related breach of this Call Off Agreement (or any other agreement between the Authority and the Contractor) by the Contractor caused or contributed to the Authority Cause; and/or

4.2.2 the Authority gives any advance notification that the Authority Cause is or is likely to occur,

then the compensation amount payable pursuant to Paragraph 4.1 above shall be reduced by a fair and equitable amount.

5. Royalty Share

5.1 If applicable, the Royalty Share Amount referred to in Clause 38.6 of the Framework Agreement shall be agreed between the Parties pursuant to the Change Control Procedure. It shall be calculated as a percentage of the gross revenue received by the Contractor from the commercial exploitation of the Specially Written Software and/or the Project Specific IPRs.

5.2 All costs associated with the Royalty Share Amount shall be shown separately in the Financial Model such that the gross revenue received by the Contractor is shown.

5.3 The Royalty Share Amount shall be paid to the Authority annually in arrears within three (3) calendar months of the relevant date of approval by the Authority.

6. Delay Payments

6.1 If a Milestone has not been achieved by the relevant Milestone Date, the Contractor shall pay to the Authority Delay Payments in accordance with the following table for each day of delay from and including the relevant Milestone Date until and including the date on which the relevant Milestone criteria are actually Achieved and the Authority provides the Contractor with a Milestone Achievement Certificate.

Milestone Number	**Delay Payment**
None	

6.2 The liability of the Contractor in respect of Delay Payments will be limited in accordance with Clause 55.2.6 (Limitations on Liability) of the Framework Agreement.

7. Charges for Change Control

7.1 The Contractor shall use the Financial Model to demonstrate any proposed revisions to the Charges arising as a result of any proposed Change.

7.2 Where a Change is requested the Contractor will prepare a quotation for the cost of the Change which shall:

7.2.1 be based on and reflect the principles of the Financial Model;

7.2.2 include estimated volumes of each type of resource to be employed and the applicable rate card specified in Appendix 2 to this Annex;

7.2.3 include full disclosure of any assumptions underlying such quotation; and

7.2.4 include evidence of the cost of any assets required for the Change.

7.3 If the Change is adopted by the Authority in accordance with Part A of Schedule 8.2 (Change Control Procedure and Call-Off Process) then the Contractor will update the Financial Model in accordance with the provisions of Schedule 7.5 (Financial Model).

7.4 Any Changes to the Charges shall be developed and agreed by the Parties such that the Contractor's profit margin on such Changes shall be no greater than that applying to the Charges on the date that the relevant Changes are agreed.

8. Indexation

8.1 Indexation shall not apply to any Milestone Payments but shall apply to Fixed Charges and any applicable Day Rate Cards.

8.2 Any amounts or sums in this Call Off Agreement which are expressed to be "subject to indexation" shall be adjusted to reflect the effects of inflation after that date in accordance with the provisions of this Paragraph. The adjustment shall be measured by changes in the relevant index published for that Contract Year as calculated in accordance with the following formula:

$$\text{Amount or Sum} \times \left(\left(\frac{Index_{o}}{Index_{d}} \right) - Y\% \right)$$

Where:

"**Index**" means Services Sector Prices Index (SSPI) '6150770000 - Administrative and Support';

"**Index** $_{d}$" is the value of Index published or determined with respect for the period immediately preceding the Effective Date;

"**Index** $_{o}$" is the value of Index published or determined with respect to the period immediately preceding the relevant anniversary in respect of which the amount or sum falls to be adjusted; and

"**Y**" is an efficiency factor of 1.0%.

9. Service Credits

9.1 The Contractor shall issue the Authority with a credit note for an amount equivalent to any Service Credits which accrue in any Measurement Period in accordance with Paragraph 4 of Part A of Schedule 2.2 (Service Levels and Service Credits). Any such Service Credits shall be credited against the invoice relating to the next month. If no further Charges fall due after Service Credits accrue, the Contractor shall issue a credit note to the Authority for a sum equal to any such Service Credits then outstanding which shall be repayable by the Contractor to the Authority as a debt, in which case the Authority shall invoice the Contractor for the sum due.

10. Time and Materials

10.1 Charges for Additional Services which are to be calculated on the basis of a "Time and Materials Charge", shall be calculated by applying the Day Rate Card specified in Appendix 2 in accordance with this Paragraph 10.1 provided that in no event shall the rates applicable to a Time and Materials Charge exceed the rates set out in the Day Rate Card set out in the Appendix to this Annex 7.1 (Charges and Invoicing).

10.2 The Contractor shall provide a breakdown of any Time and Materials Charge. For the avoidance of doubt, no risks or contingencies shall apply to the provision of Additional Services for which Time and Materials Charges apply.

10.3 The Contractor shall keep records of hours worked in the form of timesheets and expenses incurred, and it shall submit a summary of the relevant records with the invoice. The Contractor shall make available copies of the detailed records to the Authority within twenty (20) Working Days after the Authority's request.

10.4 Subject to Paragraph 2 of Appendix 2 to this Annex, the Contractor may not recover any travel, subsistence or other expense costs incurred for travel in the course of the Contractor's provision of Services.

10.5 The Contractor shall be entitled to raise an invoice in respect of any Time and Materials Charges in accordance with Paragraph 2 of Part B to this Annex.

10.6 The Parties agree that this Paragraph 10 shall not apply to any Fixed Charges and may not be used to vary the Charges for Core Services or Optional Services in any way.

PART B - INVOICING

1. Purpose of this Part B of this Annex

This Part B of this Annex sets out the method by which the Contractor shall raise invoices to the Authority for payment, together with the requirements which apply to such invoices, and the payment terms thereof.

2. Contractor Invoices

2.1 The Contractor shall be entitled to raise an invoice in respect of any payment which falls payable to the Contractor pursuant to this Call Off Agreement.

2.2 The Contractor shall provide reporting data via CSV file using the template set out in Appendix 3 of this Annex as well as a PDF invoice so invoices can be automatically reconciled by the Authority systems.

2.3 The Contractor shall invoice the Authority in respect of Services in accordance with the timescales specified for issue of invoices for the Charges as detailed in Part A of this Annex.

2.4 The Contractor shall ensure that each invoice contains the following information:

2.4.1 the date of the invoice;

2.4.2 a unique invoice number;

2.4.3 the Invoicing Period or other period(s) to which the relevant Charge(s) relate;

2.4.4 the reference number of the purchase order to which it relates (if any);

2.4.5 the dates between which the Services which are the subject of each of the Charges detailed on the invoice were performed;

2.4.6 a breakdown of the Services to which each of the Charges detailed on the invoice relate;

2.4.7 details of the number and type of transactions performed during the applicable Invoicing Period to which an invoice relates;

2.4.8 the methodology applied to calculate the Charges;

2.4.9 any payments due in respect of Achievement of a Milestone;

2.4.10 the total Charges gross and net of any applicable deductions and, separately, the amount of any disbursements properly chargeable to the Authority under the terms of this Call Off Agreement, and, separately, any VAT or other sales tax payable in respect of the same;

2.4.11 details of any Delay Payments or similar deductions that shall apply to the Charges detailed on the invoice;

2.4.12 reference to any reports required by the Authority in respect of the Services to which the Charges detailed on the invoice relate (or in the case of reports issued by the Contractor for validation by the Authority, then to any such reports as are validated by the Authority in respect of the Services);

2.4.13 a contact name and telephone number of a responsible person in the Contractor's finance department in the event of administrative queries; and

2.4.14 the banking details for payment to the Contractor via electronic transfer of funds (i.e. name and address of bank, sort code, account name and number).

2.5 In respect of each invoice, the Contractor shall supply to the Authority electronically (as soon as practicable prior to the issue of such invoice) sufficient information (**"Supporting Documentation"**) to enable the Authority to reasonably assess whether the Charges detailed thereon are properly payable. Any such assessment by the Authority shall not be conclusive. The Supporting Documentation shall be provided by the Contractor to such persons as the Authority may notify to the Contractor from time to time for internal review purposes only. The Contractor undertakes to provide to the Authority any other documentation reasonably required by the Authority from time to time to substantiate an invoice.

2.6 The Contractor shall issue invoices to the Authority by email.

2.7 Notwithstanding Paragraphs 2.5 and 2.6 above, the Contractor shall (where requested by the Authority) submit invoices and Supporting Documentation in such format as the Authority may specify from time to time to:

Recipient	Address
Cabinet Office, 1 Horse Guards Road, London, SW1A 2HQ	di-invoices@digital.cabinet-office.gov.uk
GDS, The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS	GDSBusinessOps@digital.cabinet-office.gov.uk
Cabinet Office and Shared Service Connected Limited (SSCL) PO Box 405, Phoenix House, Celtic Springs Business Park, Newport, NP10 8FZ	apinvoices-cab-u@gov.sscl.com

with a copy (again including any Supporting Documentation) to such other person and at such place as the Authority may notify to the Contractor from time to time.

2.8 All Contractor invoices shall be expressed in sterling or such other currency as shall be permitted by the Authority in writing.

2.9 The Authority shall only regard an invoice as valid if it complies with the provisions of this Part B of this Annex. Where any invoice does not conform to the Authority's requirements set out in Paragraph 2 of Part B to this Annex, the Authority will return the disputed invoice to the Contractor. The Contractor shall promptly issue a replacement invoice which shall comply with the same.

3. Payment Terms

Subject to the provisions of Paragraph 2 of Part B to this Annex, the Authority shall make payment to the Contractor within 30 days of receipt of a valid invoice by the Authority at its nominated address for invoices.

4. **Additional Payment and Invoicing Requirements**

4.1 The Contractor shall comply with the additional payment and invoicing requirements set out in this Paragraph 4.

4.2 The Contractor shall have the ability to support payment options, with no additional charge, as directed by the Authority to include, but not limited to:

- Consolidated invoice accounts, for example 7 or 30 days
- Individual and or single bill back (for example not consolidated)
- Manual invoicing
- Invoicing to different levels of detail

4.3 The Contractor will issue valid electronic invoices monthly in arrears. Each invoice shall be accompanied by a breakdown of the deliverables and services, quantity thereof, applicable unit charges and total charge for the invoice period, in sufficient detail to enable the Authority to validate the invoice. The Contractor shall ensure the invoice has the PO number and WP2087.

4.4 Where requested by the Authority the Contractor shall interface with the Contractor's payment/purchase system.

4.5 The Contractor must have a solution to accurately account for payments received when delivering the services under this Call Off Agreement. These records must be secure and retrievable within 5 Working Days upon request by the Authority.

4.6 If applicable during the term of this Call Off Agreement and where requested by the Authority, the Contractor shall agree with the Authority how to transfer any payments received in delivering the services, but at a minimum the Contractor must have UK based accounting facilities which enable the transfer of funds into an account of the Authority’s choice. Payment shall be transferred daily or at a frequency specified by the Authority.

4.7 The Contractor shall respond to any queries in relation to the remittance for services and/or upon receipt of a reconciliation report from the Authority within 5 Working Days.

4.8 The Contractor shall comply with the Authority’s requirements in respect of authorisation, invoicing and payment processes and procedures.

4.9 Invoices shall be created in line with the Authority’s requirements but at a minimum they must contain itemised charges for service provided and rates applied.

Appendix 1 – Milestone Payments and Service Charges

The table below sets out details of the transaction price, the implementation / integration charges, the ongoing charges and the expansion programme charges.

Reference Number	Description	Year 1	Year 2	Year 3	Year 4 (optional extension)	Year 5 (optional extension)	Notes	
1	**Cost per single transaction, (indicative ranges)**							Transactional service price of £11.00 is based on £7.50 IBV base fee, £1 back office & security centre checks required for GPG45, £2.50 for UK restricted processing. It covers all service costs including:
								- Hardware costs
								- Software costs including licensing
								- Postmaster staff costs
								- Post Office branch overheads
								- Postmaster training
								- Yoti UK Security centre staff costs
								- Yoti Security centre office overheads
								- Contract management costs
1.1	1– 500,000 per transaction	£11	£11	£11	£11	£11	Transaction rate only valid with minimum volume guarantee of:	- Service management costs
							Years 1-2: 200,000 transactions over 24 months (25,000 transactions per quarter)	- MI
							Year 3: 100,000 transactions over 12 months (25,000 transactions per quarter)	- Invoicing

Reference Number	Description	Year 1	Year 2	Year 3	Year 4 (optional extension)	Year 5 (optional extension)	Notes	
							Year 4: 100,000 transactions over 12 months (assuming extension) (25,000 transactions per quarter)	
							Year 5: 100,000 transactions over 12 months (assuming extension) (25,000 transactions per quarter)	
1.2	500,001 - 1,000,0000 per transaction	£11	£11	£11	£11	£11	Minimum volume guarantee required due to GDS bespoke requirement for UK only run and managed service which requires the scaling of the staffing of the UK security centre.	
1.3	1,000,001 and above per transaction	£11	£11	£11	£11	£11	IBV is a commodity service platform used by many Post Office clients. As such we are able to offer flat pricing structure for economic efficiencies and therefore there are no volume bands for the pricing of this service.	
2	**Implementation / Integration Costs**							

Reference Number	Description	Year 1	Year 2	Year 3	Year 4 (optional extension)	Year 5 (optional extension)	Notes	
2.1	Implementation costs	£35,000					Accounting for the specific development required to the service to meet GDS' requirements.	To be paid split across two miletones:
							Delivery timelines are shown in the Outline Implementation Plan.	50%: Effective Date
								50%: Service go-live
2.2	Solution Integration costs	£140,000					These costs cover the integration, testing and project management from contract award through to live service.	To be paid split across two
							Delivery timelines are shown in the Outline Implementation Plan.	miletones:
								50%: Effective Date
								50%: Service go-live
3	**Ongoing Costs**						All on-going annual costs are accounted for within the per transaction cost.	
3.1	Branch Costs	£0	£0	£0	£0	£0	All branch costs are included in transaction fee.	
3.2	Management Costs	£0	£0	£0	£0	£0	All management costs are included in transaction fee.	
3.3	(CCS) FOCS Contract Costs	£0	£0	£0	£0	£0	No CCS FOCS contract costs.	

Reference Number	Description	Year 1	Year 2	Year 3	Year 4 (optional extension)	Year 5 (optional extension)	Notes	
3.4	Reporting/MI Costs	£0	£0	£0	£0	£0	All reporting/MI costs as per requirements are included in implementation costs for set-up of reports and transaction fee for the regular supply of reports. New reporting requirements will be subject to change control process.	
3.5	Training Costs to include on-going training costs and training materials	£0	£0	£0	£0	£0	All training costs (Postmasters & security centre staff) are included in transaction fee.	
4	**Expansion Programme Costs**						Costs are presented per branch expansion. These costs are approximate, at the point of expansion request, analysis of the most suitable branches will be run and a bespoke proposal submitted.	

Reference Number	Description	Year 1	Year 2	Year 3	Year 4 (optional extension)	Year 5 (optional extension)	Notes	
4.1	Year 1	£5,900					£900/branch for expansion to cover new branch set up, infrastructure and training. £5,000 project management costs. Note - project management costs are per expansion project and not per branch. Exact value will vary depending on how many branches were included and the breadth of their locations with economies of scale applied.	Where no transactions take place in a single month or where there are less than 24 transactions in a quarter this triggers refresher training to occur for all staff within that branch to ensure quality of service.
								The cost of refresher is training is £25/branch.
								Payment would take place quarterly.
4.2	Year 2	£600					Annual service management cost payable to cover service support, device support, licenses, network connectivity, device lifecycle replacement and training.	Where no transactions take place in a single month or where there are less than 24 transactions in a quarter this triggers refresher training to occur for all staff within that branch to ensure quality of service.
								The cost of refresher is training is £25/branch.

Reference Number	Description	Year 1	Year 2	Year 3	Year 4 (optional extension)	Year 5 (optional extension)	Notes	
								Payment would take place quarterly.
4.3	Year 3	£600					Annual service management cost payable to cover service support, device support, licenses, network connectivity, device lifecycle replacement and training.	Where no transactions take place in a single month or where there are less than 24 transactions in a quarter this triggers refresher training to occur for all staff within that branch to ensure quality of service.
								The cost of refresher is training is £25/branch.
								Payment would take place quarterly.
5	The total 3-year cost will be evaluated exclusive of VAT							
	Forecast volumes	333,333.33	500,000.00	250,000.00				
5.1	Use the Authorities volumetrics to provide costs for a 3-year contract	£3,841,667	£5,500,000	£2,750,000			Assumed 01 May 23 commencement. Lower values of forecasts used for modelling. No expansion costs included.	
	Write three-year contract value in pounds and pence.							
	£12,091,667						Assumed no branch expansion	
Notes:								
1	Costs exclude VAT							
2	Transaction costs subject to indexation in accordance with paragraph 8 of this Annex.							
3	Service enhancements specifically requested and accepted for Authority during contract term will be subject to change control process							

Reference Number	Description	Year 1	Year 2	Year 3	Year 4 (optional extension)	Year 5 (optional extension)	Notes	
4	Transaction rate for ‘unavailable’ outcome transactions is £0/transaction.							

Appendix 2 – Day Rate Card

1. The Day Rate Card sets out the maximum Day Rate Cost which shall apply to each individual member of Contractor Personnel.

2. The Day Rate Card is exclusive of any travel, subsistence and expense costs incurred for travel in the course of the Contractor's preparation of any Impact Assessment within the United Kingdom. For the avoidance of doubt, where approved by the Authority, any such costs will be reimbursed by the Authority separately to the Day Rate Card rates provided in this Appendix in accordance with the Authority's then current travel and subsistence rates.

3. Day Rate Card

Job Title	Day Rate (£)
Project Manager – Experienced PRINCE II (or equivalent) qualified Project Manager	£750
Systems Developer Technical Support – Qualified Development / technical support specialist with demonstrable track record in required activity.	£1000
Business Analyst Consultant – Experienced management consultant, Management Information Analyst, Business Process Analyst capable of delivering impact assessments for change control processes.	£750
Project Team Member - Experienced and suitably Qualified Project Team member.	£500
Administration Staff Member - Experienced individual to carry out administration tasks.	£500
Average Day Rate	£700

Appendix 3 – Invoice CSV Template

The agreed version of this template at the Effective Date is contained in the email sent from Rupinder Aulak, Commercial Manager of the Authority to Elinor Hull, Identity Services Director and Jason Sheehy, Identity Product Manager of the Contractor at 21:10 on 21 June 2023 which the Contractor acknowledges was received.

ANNEX 7 – FINANCIAL MODEL

The Parties agree that for the purpose of this Call Off Agreement the table set out in Appendix 1 of Annex 6 (Charges and Invoicing) shall be treated as being the Financial Model.

ANNEX 8 – KEY PERSONNEL

Name	Key Role	Responsibilities / Authorities	Phase of the project during which they will be a Key Person (Key Role Minimum Period)
Jason Sheehy	Post Office Product Manager, Identity Services	Key Post Office product point of contact Management of ongoing product related questions Aligning PO-Yoti-GDS teams	Throughout
Elinor Hull	Post Office Identity Services Director	Key Post Office contractual point of contact	Throughout
Emily Hyett	Yoti Group Product Manager	Key Yoti product point of contact Management of ongoing product related questions Aligning PO-Yoti-GDS teams	Throughout
Kiran Bali (interim)	Yoti - Interim Project Manager	Ensuring delivery is on track Ownership of project reporting and product reports for GDS	Throughout
Jason Martyres	Yoti Integration Manager	Management of all integration and delivery issues	Throughout - particularly involved during delivery and key testing phases
Carl Dawson	Yoti GDS Account Manager	Management of commercials and questions	Throughout particularly involved during initial stages

ANNEX 9 – PENSIONS

Not Used

ANNEX 10 – INSURANCE REQUIREMENTS

1. Insurance Covenants

1.1 The Contractor:

1.1.1 shall maintain the Insurances in full force and effect at all times from the Effective Date until the date which is six (6) years following the end of the Term;

1.1.2 shall not cancel the Insurances or make any material change thereto without the express written consent of the Authority, such consent not to be unreasonably withheld or delayed; and

1.1.3 may change the insurers with whom the Insurances are held on an annual basis, upon notice to the Authority at least 10 Working Days prior to any such change. In the event that such a change results in revisions to the terms or cover, Authority consent will be required before the change can be implemented, such consent not to be unreasonably withheld or delayed.

1.2 The Insurances shall be maintained on terms that are as favourable to those generally available to a prudent contractor in respect of risks insured in the international insurance market.

1.3 The Insurances shall be maintained with a reputable insurance company.

1.4 The Contractor shall procure, at no cost to the Authority, in respect of each of the public liability, employer's liability and product liability Insurances that:

1.4.1 each such Insurance shall be extended automatically to indemnify the Authority as Joint Insured to the extent of the Authority's insurable interest; and

1.4.2 the insurers of each such Insurance shall waive all rights of subrogation or action that insurers may acquire against the Authority,

provided that the Authority shall as though they were the insured under the Insurances, observe, fulfil and be subject to the terms, exclusions, conditions and endorsements of the Insurances so far as they can apply.

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

1.6 The Authority may purchase (if possible) any of the Insurances which the Contractor has failed to maintain in full force and effect pursuant to this Agreement. The

Authority may recover the premium and other costs incurred in doing so as a debt due from the Contractor.

1.7 On request from the Authority, the Contractor shall, not more than ten (10) Working Days after the Effective Date, and within fifteen (15) Working Days after the renewal of every Insurance, forward a letter from its insurance brokers who arranged the Insurances containing at least the information set out in the appendix to this Annex. The Contractor shall confirm in each covering letter that the maximum deductible in respect of any of its insurance policies is no greater than 10% (ten per cent) of the sum insured under that policy. (Where the maximum deductible value varies between insurances, these values should be added in a separate column to the table at Paragraph 2 below).

1.8 The Authority may from time to time submit a request in writing to the Contractor, demanding evidence of the existence of all Insurances, copies of all policy terms, and evidence of the timely payment of premiums (confirmation in the form of a broker's letter), including a summary of the Insurances under which the Authority is named as a Joint Insured, and the Contractor shall provide all such evidence within five (5) Working Days of such written request.

2. Insurances

Class	**Minimum Sum Insured**
Public Liability	£10,000,000 for a single event or a series of related events and £15,000,000 in the aggregate per annum
Employers Liability	£5,000,000 for a single event or a series of related events and £15,000,000 in the aggregate per annum (or such higher minimum sum(s) that may be required by law from time to time)
Professional Indemnity	£5,000,000 for a single event or a series of related events and £10,000,000 in the aggregate per annum

Appendix to Annex 10

Contents of Broker's Letter

A) Class: **PUBLIC LIABILITY**

Insurer: [*to be completed*]

Policy No: [*to be completed*]

Period: [*to be completed*]

Confirmation that the levels of Insurance are at least as required in Paragraph 2 of this Annex 10.

Confirmation that the premiums due under the terms of the policy of insurance are not (and have not previously been) in arrears as at the date of inception or renewal or as at the date of the broker's letter.

B) Class: **EMPLOYERS LIABILITY**

Insurer: [*to be completed*]

Policy No: [*to be completed*]

Period: [*to be completed*]

Confirmation that the levels of Insurance are at least as required in Paragraph 2 of this Annex 10.

Confirmation that the premiums due under the terms of the policy of insurance are not (and have not previously been) in arrears as at the date of inception or renewal or as at the date of the broker's letter.

C) Class: **PROFESSIONAL INDEMNITY**

Insurer: [*to be completed*]

Policy No: [*to be completed*]

Period: [*to be completed*]

Confirmation that the levels of Insurance are at least as required in Paragraph 2 of this Annex 10.

Confirmation that the premiums due under the terms of the policy of insurance are not (and have not previously been) in arrears as at the date of inception or renewal or as at the date of the broker's letter.

ANNEX 11 – OTHER VARIATIONS

The Parties agree to amend the Framework Agreement terms (only insofar as they are incorporated into this Call Off Agreement and not for the purpose of any other Call Off Agreement) in accordance with Clause 2.7 of the Framework Agreement, as follows:

1. Clause 57.2 shall be deleted in its entirety and replaced with the following:

   "*57.2 The Parties may by written agreement (and pending budget approval and successful contract performance) extend the Term of the Call Off Agreement by two periods of up to twelve (12) months from the end of the Initial Term (or Extension Period, as applicable). Unless the parties agree otherwise, the Charges for the Services payable in respect of any extension of the Term of the Call Off Agreement shall be the Charges applicable immediately before the end of the Initial Term (or Extension Period, as applicable).*"

2. Schedule 1 (Definitions) is amended as set out in Attachment 1 of this Annex.

3. Not used.

4. Not Used.

5. A new Clause 26A (Reporting Supply Chain Spend) shall be inserted into the Framework Agreement following Clause 26 which shall read:

   "*26A Reporting Supply Chain Spend*

   In addition to any other Management Information requirements set out in this Call-Off Agreement, where requested by the Authority the Contractor agrees that it shall, at no charge, provide timely, full, accurate and complete supply chain spend information for the purpose of Procurement Policy Note 01/18 titled Supply Chain Visibility."

6. The contents of Clause 43 (Protection of Personal Data) is deleted from the Framework Agreement and replaced in its entirety by the provisions set out in Attachment 2. A new Schedule 9.4 (Processing Personal Data) shall also be inserted in the form set out in Attachment 2.

7. Clause 50 (Security) shall be deleted in its entirety and replaced with a new Clause 50 (Security) which shall read:

   "50. The Parties shall comply with their obligations set out in Schedule 2.5 (Security Schedule)."

8. Schedule 2.5 (Security Management Plan) shall be deleted in its entirety and replaced with a new Schedule 2.5 (Security Schedule) in the form set out in Attachment 3.

9. Not Used.

10. Clause 55.2.1 shall be amended as follows:

The reference to "*43.4 (Protection of Personal Data)*" shall be replaced with a reference to "*43.14 (Processing Personal Data)*".

11. Clause 58.3.5(e) shall be amended by the inclusion of the following new Clause 58.3.5(e)(vi): "the fraud requirements set out in the Authority Requirements;".

12. The provisions in Schedule 7.4 (Financial Distress) of the Framework Agreement which refer to the Financial Ratios shall not apply in respect of this Call Off Agreement. For the avoidance of doubt (i) such provisions shall not apply in respect of the Financial Ratios only and shall otherwise apply in full where applicable; and (ii) all of the events set out in paragraphs 3.1, 4.1 and 5.1 of Schedule 7.4 shall be Financial Distress Events (in accordance with the definition of Financial Distress Event) except for events that concern Financial Ratios.

ATTACHMENT 1 TO ANNEX 11
AMENDMENTS TO SCHEDULE 1 (DEFINITIONS)

1. Schedule 1 (Definitions) shall be amended as described in this Attachment 1.

2. The following definitions shall be inserted:

"Contracts Finder"	the online government portal which allows suppliers to search for information about contracts as prescribed by Part 4 of the Public Contract Regulations 2015;
"Controller"	has the meaning given in the UK GDPR;
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach;
"DPA 2018"	the Data Protection Act 2018;
"Data Protection Impact Assessment"	an assessment by the Controller carried out in accordance with section 3 of the UK GDPR and sections 64 and 65 of the Data Protection Act 2018;
"Data Subject Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to their Personal Data;
"EEA"	European Economic Area;
"EU GDPR"	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it has effect in EU law;
"European Standard"	in relation to an electronic invoice means the European standard and any of the standards published in Commission Implementing Decision (EU) 2017/187);
"Personal Data Breach"	shall have the meaning given in the UK GDPR;
"Processor"	has the meaning given in the UK GDPR;
"Processor Personnel"	means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-processor engaged in the performance of its obligations under this Agreement;
"Protective Measures"	appropriate technical and organisational measures designed to ensure compliance with obligations of the Parties arising under Data Protection Legislation and this Agreement, which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it including those outlined in Schedule 2.5 (Security Schedule).
"SME"	an enterprise falling within the category of micro, small and medium-sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;
"Sub-processor"	any third party appointed to process Personal Data on behalf of the Contractor related to this Agreement;
"Supply Chain Transparency Report"	means the report provided by the Contractor to the Authority in the form set out in Appendix B to Schedule 8.4 (Records Provision);
"UK GDPR"	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation), as it forms part of the law of England and

	Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, together with the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019;
"VCSE"	means a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objective;

3. The following definitions shall be deleted in their entirety:

"**Authority Information Asset Owner"**	the individual as notified by the Authority to the Contractor from time to time in accordance with Appendix 1 to Schedule 2.5 (Security Schedule);
"Data Controller"	shall have the same meaning as set out in the Data Protection Act 1998;
"Data Processor"	shall have the same meaning as set out in the Data Protection Act 1998;
"Security Tests"	shall have the meaning set out in Paragraph 4.1 of Schedule 2.5 (Security Schedule);

4. The following definitions shall be amended as follows, where deletions to the original terms are shown in struck through text and additions are shown in underlined text:

"Authority Data"	(a) the data (which shall include biometric data), text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Contractor by or on behalf of the Authority; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Agreement; and (b) any Personal Data for which the Authority is the ~~Data~~ Controller;
"Data Protection Legislation"	~~the Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and~~ (i) all applicable UK law~~s and regulations~~ relating to the processing of personal data and privacy, including ~~where applicable the guidance and codes of practice issued by the Information Commissioner;~~ but not limited to the UK GDPR, and the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; and (ii) (to the extent that it may be applicable) the EU GDPR. The UK GDPR and EU GDPR are defined in section 3 of the Data Protection Act 2018;
"Data Subject"	shall have the ~~same~~ meaning ~~as set out in the Data Protection Act 1998~~ given in the UK GDPR;
"Personal Data"	shall have the ~~same~~ meaning ~~as set out in the Data Protection Act 1998~~ given in the UK GDPR;
"Security Management Plan"	the Contractor's security plan prepared pursuant to Paragraph ~~3~~6.5 of Schedule 2.5 (Security Management Plan), a~~n outline~~ template of which is set out in Annex ~~Appendix~~ 2 to Schedule 2.5 (Security Schedule);

ATTACHMENT 2 TO ANNEX 11
CLAUSE 43 AND SCHEDULE 9.4 OF THE FRAMEWORK AGREEMENT

43. **PROCESSING PERSONAL DATA**

43.1 The Parties acknowledge that for the purposes of Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor. The only processing that the Processor is authorised to do is listed in Schedule 9.4 (Processing, Personal Data & Data Subjects) by the Controller and may not be determined by the Processor. The term "processing" and any associated terms are to be read in accordance with Article 4 of the UK GDPR.

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

43.3 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:

43.3.1 a systematic description of the envisaged processing operations and the purpose of the processing;

43.3.2 an assessment of the necessity and proportionality of the processing operations in relation to the Services;

43.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

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

43.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

43.4.1 process that Personal Data only in accordance with Schedule 9.4, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

43.4.2 ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protective Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take account of the:

(a) nature of the data to be protected;

(b) harm that might result from a Data Loss Event;

(c) state of technological development; and

(d) cost of implementing any measures;

43.4.3 ensure that :

(a) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule 9.4);

(b) 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:

(i) are aware of and comply with the Processor's duties under this clause;

(ii) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

(iii) 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 this Agreement; and

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

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

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

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

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

(d) the Processor complies with its obligations under Data Protection Legislation by providing an appropriate 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

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

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

43.5 Subject to Clause 1.6, the Processor shall notify the Controller as soon as reasonably possible if it:

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

43.5.2 receives a request to rectify, block or erase any Personal Data;

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

43.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

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

43.5.6 becomes aware of a Data Loss Event.

43.6 The Processor's obligation to notify under Clause 1.5 shall include the provision of further information to the Controller, as details become available.

43.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including but not limited to promptly providing:

43.7.1 the Controller with full details and copies of the complaint, communication or request;

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

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

43.7.4 assistance as requested by the Controller following any Data Loss Event;

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

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

43.8.1 the Controller determines that the processing is not occasional;

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

43.8.3 the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

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

43.10 Each Party shall designate its own data protection officer if required by Data Protection Legislation.

43.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:

43.11.1 notify the Controller in writing of the intended Sub-processor and processing;

43.11.2 obtain the written consent of the Controller;

43.11.3 enter into a written agreement with the Sub-processor which give effect to the terms set out in this Clause 43 such that they apply to the Sub-processor; and

43.11.4 provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

43.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

43.13 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may upon giving the Processor not less than 30 working days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

43.14 The Contractor shall at all times, during and after the Term, on written demand indemnify the Authority and keep the Authority indemnified against all losses, damages, costs or expenses and other liabilities (including legal fees) incurred by, awarded against or agreed to be paid by the Authority arising from the Contractor's breach of this Clause 43.

SCHEDULE 9.4

PROCESSING, PERSONAL DATA & DATA SUBJECTS

1. The contact details of the Controller's Data Protection Officer are: Denise Dolan, Government Digital Services, Denise.Dolan@digital.cabinet-office.gov.uk
2. The contact details of the Processor's Data Protection Officer are: Chris Russell, Post Office, Data.Protection@postoffice.co.uk
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor in accordance with Clause 43.1.
Subject matter of the processing	The processing is needed in order to ensure that the Processor can effectively provide the Services.
Duration of the processing	For the duration of the Call Off Agreement.
Nature and purposes of the processing	Collection, organisation, structuring, storage, retrieval, consultation, use, disclosure and deletion of data for the purpose of providing a document/identification service for the Authority's One Login service.
Type of Personal Data being Processed	Personal identification data such as name, date of birth, address, photograph, nationality, any other information captured on relevant documents processed as part of providing the services as described in the Agreement and name of intended Post Office branch to visit.
Categories of Data Subject	Customers of the Authority.
International transfers and legal gateway	N/A

Description	Details
Plan for return and destruction of the data once the processing is complete	The information within each individual request is held according to the “TTL” (time-to-live) set by the Authority at session creation time, however a copy of the information captured during the face to face checks is retained for 28 days.

ATTACHMENT 3 TO ANNEX 11
SCHEDULE 2.5 (SECURITY MANAGEMENT PLAN)

Framework Schedule 2.5 (Security Management Plan) shall be replaced with the Security Schedule set out below.

The Contractor's compliance with the Security Schedule shall be subject to the deviations set out in Appendix 1 of Annex 3 (Contractor Solution).

Cabinet Office

GDS

Security Schedule:

(Security Management: Contractor-led Assurance)

Contents

1 Authority Options

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

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

2 Definitions

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

	(i) prevents the harmful effects of the Malicious Software; and (ii) removes the Malicious Software from the Supplier Information Management System;
”Authority Data”	as defined in Schedule 1 (Definitions) and, for the avoidance of doubt, shall include any meta data relating to categories of data referred to in paragraphs (a) or (b), the Code and any meta data relating to the Code.
“Authority Data Register”	means the register of all Authority Data the Contractor, or any Sub-contractor, receives from or creates for the Authority, produced and maintained in accordance with paragraph 15 of the Security Requirements;
”Authority Premises”	as defined in Schedule 1 (Definitions);
“Authority System”	as defined in Schedule 1 (Definitions);
“Breach Action Plan”	means a plan prepared under paragraph 14.3 of the Security Requirements addressing any Breach of Security;
“Breach of Security”	for the purposes of this Security Schedule, means the occurrence of: (a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Authority, the Contractor or any Sub-contractor in connection with this Call Off Agreement, including the Authority Data and the Code; (d) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Authority, the Contractor or any Sub-contractor in connection with this Call Off Agreement, including the Authority Data and the Code; and/or (e) any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements; (f) the installation of Malicious Software in the: (i) Supplier Information Management System; (ii) Development Environment; or (iii) Developed System; (g) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the: (i) Supplier Information Management System; (ii) Development Environment; or (iii) Developed System; and

	(h) includes any attempt to undertake the activities listed in sub-paragraph (a) where the Contractor has reasonable grounds to suspect that attempt: (i) was part of a wider effort to access information and communications technology by or on behalf of Central Government Bodies; or (ii) was undertaken, or directed by, a state other than the United Kingdom
"Certification Requirements"	means the requirements set out in paragraph 12.3.
"CHECK Scheme"	means the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks
"CHECK Service Provider"	means a company which, under the CHECK Scheme: (a) has been certified by the National Cyber Security Centre; (b) holds "Green Light" status; and (c) is authorised to provide the IT Health Check services required by paragraph 10 of the Security Requirements;
"Code"	means, in respect of the Developed System: (a) the Source code; (b) the Object code; (c) third-party components, including third-party coding frameworks and libraries; and (d) all supporting documentation.
"Code Review"	means a periodic review of the Code by manual or automated means to: (a) identify and fix any bugs; and (b) ensure the Code complies with (i) the requirements of this Security Schedule ; and (ii) the Secure Development Guidance;
"Code Review Plan"	means the document agreed with the Authority under paragraph 5.2 of the Security Requirements setting out the requirements for, and frequency of, Code Reviews;
"Code Review Report"	means a report setting out the findings of a Code Review;

"Contractor Personnel"	as defined in Schedule 1 (Definitions);
"Contractor System"	as defined in Schedule 1 (Definitions);
"Cyber Essentials"	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Plus"	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Scheme"	means the Cyber Essentials scheme operated by the National Cyber Security Centre;
"Developed System"	means any software or system that the Contractor will develop under this Call Off Agreement either: (a) as part of the Services; or (b) to create or modify Software to: (i) provide the Services; or (ii) Process Authority Data,;
"Development Activity"	means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including: (a) coding; (b) testing; (c) code storage; and (d) deployment.
"Development Environment"	means any information and communications technology system and the Sites forming part of the Supplier Information Management System that the Contractor or its Sub-contractors will use to provide the Development Activity;
"EEA"	means the European Economic Area;
"End-user Device"	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services.
"Email Service"	means a service that will send, or can be used to send, emails from the Authority's email address or otherwise on behalf of the Authority;
"Higher Risk Sub-contractor"	means a Sub-contractor that Processes Authority Data, where that data includes either: (a) the Personal Data of 1000 or more individuals in aggregate during the period between the first Operational Service Commencement Date and the date on which this Call Off Agreement terminates in accordance with Clause 4.1(b); or (b) any part of that Authority Data includes any of the following:

	(i) financial information (including any tax and/or welfare information) relating to any person; (ii) any information relating to actual or alleged criminal offences (including criminal records); (iii) any information relating to children and/or vulnerable persons; (iv) any information relating to social care; (v) any information relating to a person's current or past employment; or (vi) Special Category Personal Data; or (c) the Authority in its discretion, designates a Sub-contractor as a Higher Risk Sub-Contractor: (i) in any procurement document related to this Call Off Agreement; or (ii) during the Term;
"HMG Baseline Personnel Security Standard"	means the employment controls applied to any individual member of the Contractor Personnel that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 6.0, May 2018 (https://assets.publishing.service.gov.uk /government/uploads/system/uploads/attachment_data/file/714002/ HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf), as that document is updated from time to time;
"Independent Security Adviser"	means the independent and appropriately qualified and experienced security architect or expert appointed under Paragraph 18;
"Information Management System"	means the Supplier Information Management System and the Wider Information Management System;
"IT Health Check"	means testing of the Supplier Information Management System by a CHECK Service Provider;
International Data Transfer Agreement (IDTA's)	Replaces Standard Contract Clauses under UK GDPR for International data transfers/restricted data transfers, and processing of data outside the UK
"Malicious Software"	as defined in Schedule 1 (Definitions);
"Medium Risk Sub-contractor"	means a Sub-contractor that Processes Authority Data, where that data (a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the first Operational Service Commencement Date and the date on which this Call Off Agreement terminates in accordance with Clause 4.1(b); and (b) does not include Special Category Personal Data;
"Modules Register"	means the register of Third-party Software Modules required by paragraph 7.2 of the Security Requirements;
"NCSC"	means the National Cyber Security Centre;

“NCSC Cloud Security Principles”	means the NCSC’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles.
“NCSC Device Guidance”	means the NCSC’s document “Device Security Guidance”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;
“NCSC Protecting Bulk Personal Data Guidance”	means the NCSC’s document “Protecting Bulk Personal Data”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data
“NCSC Secure Design Principles”	means the NCSC’s document “Secure Design Principles”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cyber-security-design-principles.
“OWASP”	means the Open Web Application Security Project Foundation;
“OWASP Secure Coding Practice”	means the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content;
“OWASP Top Ten”	means the list of the most critical security risks to web applications published annually by OWASP and found at https://owasp.org/www-project-top-ten/;
“Privileged User”	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
“Process”	means any operation performed on data (which includes without limitation, Personal Data), whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data, and “Processing” shall be interpreted accordingly”;
“Prohibited Activity”	means the storage, access or Processing of Authority Data prohibited by a Prohibition Notice;
“Prohibition Notice”	means a notice issued under paragraph 1.8 of the Security Requirements.
“Protective Monitoring System”	means the system implemented by the Contractor and its Sub-contractors under paragraph 12.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Authority Data and the Code
“Register of Support Locations and Third-Party Tools”	means the part of the Security Management Plan setting out, in respect of Support Locations and Third-Party Tools:

	(a) the nature of the activity performed at the Support Location or by the Third-Party Tool on the Code or the Authority Data (as applicable); (b) where that activity is performed by individuals, the place or facility from where that activity is performed; and (c) in respect of the entity providing the Support Locations or Third-Party Tools, its: (i) full legal name; (ii) trading name (if any) (iii) country of registration; (iv) registration number (if applicable); and (v) registered address.
"Relevant Activities"	means those activities specified in paragraph 1.1 of the Security Requirements.
"Relevant Certifications"	means: (a) in the case of the Contractor, any SIMS Sub-contractor and any Sub-contractor that Processes Authority Data: (i) ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2013; and (ii) Cyber Essentials Plus; and (b) for all other Sub-contractors means Cyber Essentials Plus;
"Relevant Convictions"	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences) or any other offences relevant to Services as the Authority may specify
"Remediation Action Plan"	means the plan prepared by the Contractor in accordance with Paragraph 10.20 to 10.24, addressing the vulnerabilities and findings in a IT Health Check report
"Risk Management Approval Statement"	the statement issued by the Authority under Paragraph 15.2 following the Authority-led Assurance of the Supplier Information Management System;

“Secure Development Guidance”	means the Contractor’s secure coding policy required under its ISO27001 Relevant Certification;
“Security Management Plan”	means the document prepared in accordance with the requirements of Paragraph 13 and in the format, and containing the information, specified in Annex 2.
“Security Requirements”	mean the security requirements in Annex 1 to this Security Schedule
“Security Requirements for Development”	means the security requirement Annex 2 to this Security Schedule
"Security Test"	means: (a) an Authority Security Test; (b) an IT Health Check; or (c) a Contractor Security Test.
"Security Working Group"	means the Board established under Paragraph 8 or Schedule 8.1 (Governance), as applicable;
“SIMS Sub-contractor”	means a Sub-contractor designated by the Authority that provides or operates the whole, or a substantial part, of the Supplier Information Management System;
“Sites”	means any premises (including the Authority Premises, the Contractor’s premises or third-party premises): (a) from, to or at which: (i) the Services are (or are to be) provided; or (ii) the Contractor manages, organises or otherwise directs the provision or the use of the Services; or (b) where: (i) any part of the Supplier System is situated; or (ii) any physical interface with the Authority System takes place;
“SMP Sub-contractor”	means a Sub-contractor with significant market power, such that: (c) they will not contract other than on their own contractual terms; and (d) either: (i) there are no other substitutable suppliers of the particular services other than SMP Sub-contractors; or

	(ii) the Sub-contractor concerned has an effective monopoly on the provision of the Services.
"Statement of Information Risk Appetite"	means the statement provided by the Authority under Paragraph 7.1 setting out the nature and level of risk that the Contractor accepts from the operation of the Supplier Information Management System.
"Sub-contractor"	as defined in Schedule 1 (Definitions) and includes, for the purposes of this Security Schedule , any individual or entity that: (a) forms part of the supply chain of the Contractor; and (b) has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Authority Data;
"Sub-contractor Personnel"	means: (a) any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and (b) engaged in or likely to be engaged in: (i) the performance or management of the Services; (ii) or the provision of facilities or services that are necessary for the provision of the Services.
"Sub-contractors' Systems"	means the information and communications technology system used by a Sub-contractor in implementing and performing the Services, including: (a) the Software; (b) the Supplier Equipment; (c) configuration and management utilities; (d) calibration and testing tools; (e) and related cabling; but does not include the Authority System;
"Supplier Information Management System"	means (a) the Contractor System; (b) the Sites; (c) any part of the Authority System the Contractor or any Sub-contractor will use to Process Authority Data, or provide the Services; and (d) the associated information management system, including all relevant: (i) organisational structure diagrams, (ii) controls, (iii) policies,

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

		(ii)	controls,
		(iii)	policies,
		(iv)	practices,
		(v)	procedures,
		(vi)	processes; and
		(vii)	resources.

3 Introduction

3.1 This Security Schedule sets out:

(a) the Authority's decision on where the Contractor may:

(i) store, access or process Authority Data;

(ii) undertake the Development Activity;

(iii) host the Development Environment; and

(iv) locate Support Locations,

(in Paragraph 1)

(b) the principles of security that apply to this Call Off Agreement (in Paragraph 4);

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

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

(e) the governance arrangements for security matters, where these are not otherwise specified in Schedule 8.1 (*Governance*) (in Paragraph 8);

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

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

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

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

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

(k) the granting by the Authority of approval for the Contractor to commence:

(i) the provision of Services; and/or

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

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

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

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

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

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

4 Principles of security

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

(a) the Authority System;

(b) the Contractor System;

(c) the Sites;

(d) the Services; and

(e) the Supplier Information Management System.

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

5 Security requirements

5.1 The Contractor must, unless otherwise agreed in writing with the Authority:

(a) comply with the Security Requirements; and

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

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

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

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

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

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

6 Authority to proceed

6.1 Notwithstanding anything in this Call Off Agreement, the Contractor may not:

(a) commence the provision of any Services; or

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

unless:

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

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

(e) the Authority has provided a Risk Management Approval Statement under Paragraph 15.

7 Contractor confirmation

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

(a) the Contractor has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Call Off Agreement;

(b) subject to Paragraph 7.2:

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

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

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

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

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

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

7.3 The Contractor must:

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

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

8 Governance

8.1 This Paragraph 8 applies where a Security Working Group, or Board (as that term is defined in Schedule 8.1 (*Governance*) with a similar remit, is not provided for otherwise in this Call Off Agreement.

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

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

(a) the Authority members;

(b) the Contractor members;

(c) the chairperson of the Security Working Group;

(d) the date of the first meeting;

(e) the frequency of meetings; and

(f) the location of meetings

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

8.5 The Security Working Group meets:

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

(b) additionally when required by the Authority.

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

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

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

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

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

(a) are not binding on the Contractor; and

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

8.8 Appendix 3 applies to the Security Working Group.

9 Personnel

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

9.2 To facilitate:

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

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

at reasonable times and on reasonable notice:

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

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

10 Sub-contractors

SIMS Sub-contractor

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

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

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

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

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

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

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

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

Sub-contractors

10.4 Unless otherwise set out in Appendix 1 to Annex 3 (Contractor Solution), the Contractor must ensure that Sub-contractors comply with all Security Requirements and Security Requirements for Development that apply to the activities that the Sub-contractor performs under its Sub-contract with the Contractor.

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

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

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

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

11 Supplier Information Management System

11.1 The Contractor must determine:

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

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

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

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

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

11.5 Where a proposed change to:

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

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

is considered significant or material and has specific impact to Authority Data then such change:

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

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

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

12 Certification Requirements

12.1 The Contractor shall ensure that, unless otherwise agreed by the Authority, both:

(a) it; and

(b) any Sub-contractor,

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

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

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

(ii) Cyber Essentials Plus. It is acknowledged the Supplier is Cyber Essential Plus compliant only and the SIMS sub-contractor is not, but holds SOC 2 certification.

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

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

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

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

(a) currently in effect;

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

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

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

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

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

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

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

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

12.5 Where the Contractor has notified the Authority of a Certification Default under Paragraph 12.4:

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

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

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

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

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

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

(d) the rejection by the Authority of a revised Certification Rectification Plan is a material Default of this Call Off Agreement;

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

13 Security Management Plan

Purpose of Security Management Plan

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

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

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

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

13.3 The Contractor must ensure that:

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

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

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

Preparation of Security Management Plan

13.4 The Contractor must prepare and submit the Security Management Plan to the Authority:

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

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

13.5 If Paragraph 13.4(b) applies, and any delay resulting from the Authority's review and approval of the Security Management Plan causes or contributes to a Contractor Default, that delay is not a Authority Cause and the Contractor shall not be entitled to any relief or compensation under Clause 8.

Contents of Security Management Plan

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

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

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

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

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

(i) the Authority Premises;

(ii) the Sites;

(iii) the Contractor System;

(iv) the Authority System (to the extent that it is under the control of the Contractor); and

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

(A) in connection with this Call Off Agreement or

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

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

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

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

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

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

(i) the Sub-contractor's:

(A) legal name;

(B) trading name (if any); and

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

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

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

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

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

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

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

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

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

(k) the Modules Register;

(l) the Support Register; and

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

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

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

14 Monitoring and updating Security Management Plan

Updating Security Management Plan

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

Monitoring

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

(a) a significant change to the components or architecture of the Supplier Information Management System which relates to the manner that the Contractor processes Authority Data;

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

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

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

(i) SIMS Sub-contractor; or

(ii) Sub-contractor that Processes Authority Data;

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

(f) where the Contractor has previously Processed Authority Data that is Personal Data, not including Special Category Personal Data, it proposes to start to Process Authority Data that is Special Category Personal Data under this Call Off Agreement;

must:

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

(h) within 10 Working Days, or such other timescale as may be agreed with the Authority, update the Security Management Plan and provide the Authority with a copy of that document for review at the Security Working Group (SWG) for agreed next steps to be undertaken.

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

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

15 Review and approval of Security Management Plan

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

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

(a) where satisfied that the:

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

(ii) that the residual risks are:

(A) either:

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

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

(B) understood and accepted by the Authority; and

(C) recorded in the Residual Risk Statement;

a Risk Management Approval Statement; or

(b) where the Authority considers that:

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

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

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

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

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

16 Changes to the Supplier Information Management System

16.1 Notwithstanding anything in this Call Off Agreement, the Contractor must advise the Authority via the SWG process to agree next steps before making any of the following changes to the Supplier Information Management System:

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

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

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

(i) SIMS Sub-contractor; or

(ii) Sub-contractor that Processes Authority Data.

16.2 In seeking the Authority's approval to a proposed changes to the Supplier Information Management System where this impacts Authority Data, the Contractor must:

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

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

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

(iii) a risk assessment of the proposed change; and

(b) where this impacts Authority Data, provide that proposal to the Authority no later than 30 Working Days before the date on which the Contractor proposes to implement those changes.

16.3 The Authority:

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

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

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

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

(c) must not:

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

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

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

Implementation of changes

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

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

(a) that failure is a material Default; and

(b) the Contractor shall:

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

(A) until the Default is remedied, or

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

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

17 Remediation Action Plan

Preparation of Remediation Action Plan

17.1 Where:

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

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

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

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

(a) how the matter will be remedied;

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

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

Consideration of Remediation Action Plan

17.3 The Contractor must

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

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

Implementing an approved Remediation Action Plan

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

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

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

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

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

18 Independent Security Adviser

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

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

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

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

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

(a) a person selected by the Contractor and approved by the Authority; or

(b) where

(i) the Authority does not approve the persons selected by the Contractor; or

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

a person selected by the Authority.

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

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

(b) provide advice and recommendations on:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18.6 The Contractor shall be responsible for:

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

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

18.7 If the Contractor or any relevant Sub-contractor:

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

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

this is a material Default that is capable of remedy.

19 Withholding of Charges

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

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

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

(i) the Authority is entitled to terminate the Call Off Agreement for material Default on any of the grounds set out in Clause 58.3.5; or

(ii) the Contractor commits a material Default that is capable of remedy and the Authority is entitled to step-in pursuant to Clause 63.1.

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

19.3 Before withholding any Charges under Paragraph 19.1 the Authority must

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

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

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

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

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

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

(b) consider any representations that the Contractor may make concerning the Authority's decision.

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

19.5 The Contractor acknowledges:

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

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

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

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

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

20 Access to Authority System

Where the Contractor, a Sub-contractor or any of the Contractor Personnel is granted access to the Authority System or to the Authority Equipment, it must comply with and ensure that all such Sub-contractors and Contractor Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Authority System or the Authority Equipment.

21 Additional standards

The Contractor shall (and shall ensure that its Sub-contractors shall) comply with where applicable:

(a) The Government Technology Code of Practice (https://www.gov.uk/government/publications/technology-code-of -practice)

(b) The Government Service Standard and Service Manual (https://www.gov.uk/service-manual/service-standard)

(c) NCSC Cyber Assessment Framework Guidance https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

(d) NCSC guidance https://www.ncsc.gov.uk/section/advice-guidance/all-topics

(e) Government Functional Security Standard No.7 https://www.gov.uk/government/publications/government-functional-standard-govs-007-security

(f) NCSC Cloud Security Principles; https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

(g) Cyber Essentials plus certification

Appendix 1 Security Requirements

1. Location

Location for Relevant Activities

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

(a) store, access or process Authority Data;

(b) undertake the Development Activity; and

(c) host the Development Environment,

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

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

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

(a) the entity has entered into a binding Call Off Agreement with the Contractor or Sub-contractor (as applicable);

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

(c) the Contractor or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding Call Off Agreement;

(d) the Contractor has provided the Authority with such information as the Authority requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

(iii) the entity's compliance with the binding Call Off Agreement; and

(e) the Authority has not given the Contractor a Prohibition Notice under paragraph 1.8.

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

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

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

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

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

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

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

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

Support Locations

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

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

(a) the entity has entered into a binding Call Off Agreement with the Contractor or Sub-contractor (as applicable);

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

(c) the Contractor or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding Call Off Agreement;

(d) the Contractor has provided the Authority with such information as the Authority requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

(iii) the entity's compliance with the binding Call Off Agreement; and

(iv) the Authority has not given the Contractor a Prohibition Notice under paragraph 1.8.

Third-party Tools

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

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

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

1.7.2 a new Third-party Tool, or replace an existing Third-party Tool, without advising the Authority.

Prohibited Activities

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

1.8.1 in any particular country or group of countries;

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

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

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

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

1.10 Nothing in this Paragraph 1 shall affect the Parties obligations to comply with Clause 43.4.4 and the conditions set out therein shall continue to apply in addition to the requirements of this Paragraph 1.

2. Vetting, Training and Staff Access

Vetting before performing or managing Services

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

2.1.1 Development Activity;

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

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

unless:

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

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

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

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

2.2.1.1 the individual's identity;

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

2.2.1.3 the individual's previous employment history; and

2.2.1.4 that the individual has no Relevant Convictions;

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

2.2.3 such other checks for the Contractor Personnel of Sub-contractors as the Authority may specify.

Annual training

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

2.3.1 General training concerning security and data handling; and

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

Staff access

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

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

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

Exception for certain Sub-contractors

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

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

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

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

3. End-user Devices

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

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

3.1.2 users must authenticate before gaining access;

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

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

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

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

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

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

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

4. Hardware and software support

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

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

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

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

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

4.4 The Contractor must:

4.4.1 review and update the Support Register:

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

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

4.4.1.3 at least once every 12 months;

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

4.4.2.1 whenever it updates the Support Register; and

4.4.2.2 otherwise when the Authority requests.

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

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

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

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

4.6.1 regular firmware updates to the hardware; and

4.6.2 a physical repair or replacement service for the hardware.

5. Encryption

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

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

5.3 Notwithstanding anything in the specification for the Developed System or this Call Off Agreement, the Contractor must ensure that the Developed System encrypts Authority Data:

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

5.3.2 when the Authority Data is transmitted.

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

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

5.4.2 when transmitted.

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

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

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

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

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

5.7 Where the Authority and Contractor reach agreement, the Contractor must update the Security Management Plan to include:

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

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

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

6. Not Used

7. Not Used

8. Malicious Software

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

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

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

8.2.2 is configured to perform automatic software and definition updates;

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

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

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

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

8.4 The Contractor must at all times, during and after the Term (subject to the Limitation Act 1980), on written demand indemnify the Authority and keep the Authority indemnified, against all Losses incurred by, awarded against or agreed to be paid by the Authority arising from any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Contractor, or a Sub-contractor, to comply with this paragraph.

9. Vulnerabilities

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

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

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

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

9.2 The Contractor must:

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

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

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

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

9.3.1.2 Microsoft's security bulletin severity rating system.

10. Security testing

Responsibility for security testing

10.1 The Contractor is solely responsible for:

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

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

Security tests by Authority

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

10.3 Where the Authority gives notice under paragraph 10.2:

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

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

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

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

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

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

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

10.4 In addition to its rights under paragraph 10.2, the Authority and/or its authorised representatives may, at any time and with notice to the Contractor, carry out such tests (including penetration tests) as it may deem necessary in relation to:

(a) the Service;

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

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

("**Authority Security Tests**").

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

10.6 The Authority shall notify the Contractor of the results of such Authority Security Tests after completion of each Authority Security Test.

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

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

Security tests by Contractor

10.9 The Contractor must:

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

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

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

undertake the following activities:

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

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

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

(a) any Remediation Action Plan;

(b) the ISO27001 Certification Requirements;

(c) the Security Management Plan; and

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

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

10.11 The Contractor must

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

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

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

10.13 Not Used.

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

IT Health Checks

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

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

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

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

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

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

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

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

Remedying vulnerabilities

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

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

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

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

10.19 The Contractor must notify the Authority without undue delay if it does not, or considers it will not be able to, remedy the vulnerabilities classified as critical, high or medium in a Security Test report within the time periods specified in Paragraph 10.18.

Responding to a Security Test report

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

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

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

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

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

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

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

10.24 Where a Remediation Action Plan is deemed by the Authority to be insufficient then the SWG may request additional actions to be agreed jointly between parties, to address:

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

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

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

10.25 Where the Authority accepts the draft Remediation Action Plan, the Contractor must immediately start work on implementing the Remediation Action Plan in accordance with Paragraph 10.26 and 10.27.

Implementing an approved Remediation Action Plan

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

10.27 If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Contractor shall without undue delay of becoming aware of such risk, threat, vulnerability or exploitation technique:

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

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

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

Significant vulnerabilities

10.28 Where:

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

(b) the Authority does not accept a revised draft Remediation Action Plan,

the Authority may, at the Contractor's cost, either:

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

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

11. Access Control

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

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

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

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

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

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

11.2.1 are allocated to a single, individual user;

11.2.2 are accessible only from dedicated End-user Devices;

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

11.2.4 require passwords with high complexity that are changed regularly;

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

11.2.6 are:

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

11.2.6.2 time limited; and

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

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

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

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

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

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

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

12. Event logging and protective monitoring

Protective Monitoring System

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

12.1.1 identify and prevent potential Breaches of Security;

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

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

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

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

12.2 The Protective Monitoring System must provide for:

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

12.2.2 regular reports and alerts to identify:

12.2.2.1 changing access trends;

12.2.2.2 unusual usage patterns; or

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

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

12.2.4 any other matters required by the Security Management Plan.

Event logs

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

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

12.3.2 sensitive data, such as credentials or security keys.

Provision of information to Authority

12.4 The Contractor must provide the Authority on request with:

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

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

Changes to Protective Monitoring System

12.5 The Authority may at any time require the Contractor to update the Protective Monitoring System to:

12.5.1 respond to a specific threat identified by the Authority;

12.5.2 implement additional audit and monitoring requirements; and

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

13. Audit rights

Right of audit

13.1 The Authority may undertake an audit of the Contractor or any Sub-contractor to:

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

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

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

13.1.4 review the integrity and security of the Code.

13.2 Any audit undertaken under this Paragraph 13.1:

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

13.2.2 is in addition to and without prejudice to any other rights of audit the Authority has under this Contract (including but not limited to, Clause 33).

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

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

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

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

13.3.3.1 an IT Health Check; or

13.3.3.2 a Breach of Security.

Conduct of audits

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

13.5 The Authority must when conducting an audit:

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

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

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

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

13.6.2 access to the Supplier Information Management System; and

13.6.3 access to the Contractor Personnel.

Response to audit findings

13.7 Where an audit finds that:

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

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

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

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

14. Breach of Security

Reporting Breach of Security

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

Immediate steps

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

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

14.2.2 remedy such Breach of Security to the extent possible;

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

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

Subsequent action

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

14.3.1 full details of the Breach of Security; and

14.3.2 if required by the Authority:

14.3.2.1 a root cause analysis; and

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

1. (the “Breach Action Plan”).

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

14.4.1 how the issue will be remedied;

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

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

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

14.6 The Authority may:

14.6.1 not endorse the draft Breach Action Plan where it considers that the draft Breach Action Plan is inadequate, providing its reasons for doing so, in which case:

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

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

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

Assistance to Authority

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

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

Reporting of Breach of Security to regulator

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

14.9.1 make that report within the time limits:

14.9.1.1 specified by the relevant regulator; or

14.9.1.2 otherwise required by Law;

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

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

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

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

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

15. Return and Deletion of Authority Data

15.1 The Contractor must create and maintain a register of

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

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

15.2 The Contractor must:

15.2.1 review and update the Authority Data Register:

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

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

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

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

15.2.2.1 whenever it updates the Authority Data Register; and

15.2.2.2 otherwise when the Authority requests.

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

15.3.1 when requested to do so by the Authority; and

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

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

15.4.1 when requested to do so by the Authority; and

15.4.2 using the method specified by the Authority.

Appendix 2 Security Requirements for Development

1. Secure Software Development by Design

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

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

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

1.1.2.1 in unforeseen circumstances; and

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

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

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

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

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

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

1.3.1.1 trained and experienced in secure by design code development;

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

1.3.2 ensure that all Code:

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

1.3.2.2 follows OWASP Secure Coding Practice

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

1.3.2.4 employs consistent naming conventions;

1.3.2.5 is coded in a consistent manner and style;

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

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

(a) any original coding; and

(b) at any time the Code is changed;

1.3.3 ensure that all Development Environments:

1.3.3.1 protect access credentials and secret keys;

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

1.3.3.3 requires multi-factor authentication to access;

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

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

2. Secure Architecture

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

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

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

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

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

3. Code Repository and Deployment Pipeline

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

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

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

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

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

4. Development and Testing Data

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

5. Code Reviews

5.1 The Contractor must:

5.1.1 regularly; or

5.1.2 as required by the Authority

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

5.2 Before conducting any Code Review, the Contractor must agree with the Authority:

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

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

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

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

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

5.4 The Contractor:

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

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

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

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

5.6.1 remedy these at its own cost and expense;

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

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

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

6. Third-party Software

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

7. Third-party Software Modules

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

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

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

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

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

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

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

7.3.1 full details of the developer of the module;

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

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

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

7.4 The Contractor must:

7.4.1 review and update the Modules Register:

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

7.4.1.2 at least once every 6 (six) months;

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

7.4.2.1 whenever it updates the Modules Register; and

7.4.2.2 otherwise when the Authority requests.

Appendix 3 Security Working Group

1 Role of the Security Working Group

1.1 The Security Working Group shall be responsible for the ongoing management, maintenance, monitoring and enhancement of the Contractor's security posture in line with the contractual obligations set out in the Security Schedule.

1.2 The Security Working Group:

(a) monitors and provides recommendations to the Contractor on the Authority-led assurance of the Supplier Information Management System;

(b) builds a collaborative and robust working relationship between the Contractor and Service;

(c) reviews and monitors the design implementation involving the Contractor, and application of safety management systems, including cyber and fraud frameworks in all Digital Identity related aspects of service and design principles;

(d) reports (by exception) on risks to Board level where and when appropriate;

(e) monitors and supports mitigation of risk to systems and services for the Digital Identity evolution of service and standards, including risk exposures, risk posture and appetite, with a view to emerging and unknown risks; and

(f) oversees and aligns the operations of the Contractor to observe secure architecture standards and security due diligence.

2 Meetings of the Security Working Group

2.1 Paragraphs 3.4 to 3.7 of Schedule 8.1 (Governance) shall apply to the Security Working Group as if it were a Board established under that Schedule.

3 Reports to the Security Working Group

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

(a) ITHC and/or penetration testing reports;

(b) remediation action plans relevant to this Call Off Agreement;

(c) latest risk register relevant to this Call Off Agreement;

(d) incident reports relevant to this Call Off Agreement; and

(e) threat analysis relevant to this Call Off Agreement.

4 Administration

4.1 The Contractor is responsible for the secretarial functions of the Security Working Group.

Appendix 4 Not Used

Appendix 5 Security Management Plan Template

Copy of Security Management Plan Template May23 - Google Docs