HM Revenue & Customs

HMRC Tier 1 and 2 Model ICT Contract
Version 2.3 (December 2020)

SCHEDULE 1 | Definitions

OFFICIAL - SENSITIVE - COMMERCIAL

SCHEDULE 1 | Definitions

Unless otherwise provided or the context otherwise requires the following expressions shall have the meanings set out below.

"Accounting Reference Date"	means in each year the date to which the Supplier prepares its annual audited financial statements;
"Achieve"	(a) in respect of a Test, to successfully pass a Test without any Test Issues; and (b) in respect of a Milestone, to successfully complete a Milestone in accordance with the provisions of Schedule 6.2 (*Testing Procedures*), and **"Achieved"** and **"Achievement"** shall be construed accordingly;
"Acquired Rights Directive"	the European Council Directive 77/187/EEC on the approximation of laws of European member states relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses, as amended or re-enacted from time to time;
"Admission Agreement"	has the meaning given in Schedule 9.1 (*Staff Transfer*);
"Affected Party"	the Party seeking to claim relief in respect of a Force Majeure Event;
"Affiliate"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;
"Agreement" or "Contract"	means the clauses of this agreement together with the Schedules and annexes to it;
"Allowable Assumptions"	the assumptions set out in Annex 5 of Schedule 7.1 (*Charges and Invoicing*);
"Allowable Price"	in relation to the Retained Deliverables relating to a CPP Milestone, if any, an amount determined in accordance with the formula: A – B where: (a) A is an amount equal to the Costs incurred by the Supplier in providing or developing the relevant

Retained Deliverables as reflected in the Financial Model together with an amount equal to the Anticipated Contract Life Profit Margin thereon; and

(b) B is an amount equal to the Allowable Price Adjustment relating to the relevant Retained Deliverables, if any, or if there is no such Allowable Price Adjustment, zero,

provided that the Allowable Price for any Retained Deliverables shall in no circumstances exceed the aggregate amount of the Milestone Payments paid to the Supplier in respect of the Milestones (or in the case of Partial Termination, the Milestones for the parts of the Services terminated) relating to that CPP Milestone;

"Allowable Price Adjustment" has the meaning given in Clause **Error! Reference source not found.** (*Payments by the Supplier*);

"Annual Contract Report" has the meaning given in Schedule 7.5 (*Financial Reports and Audit Rights*);

"Annual Revenue" means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology:

(a) figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12-month period; and

(b) where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date;

"Anticipated Contract Life Profit Margin" has the meaning given in Schedule 7.1 (*Charges and Invoicing*);

"Approved Sub-Licensee"	any of the following: (a) a Central Government Body; (b) any third party providing services to a Central Government Body; and/or (c) any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Authority;
"Assets"	all assets and rights used by the Supplier to provide the Services in accordance with this Agreement but excluding the Authority Assets;
"Associated Person"	has the meaning set out at Section 44(4) of the Criminal Finances Act 2017;
"Associates"	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles;
"Assurance"	means written confirmation from a Relevant Authority to the Supplier that the CRP Information is approved by the Relevant Authority;
"ATP Milestone"	the Milestone linked to Authority to Proceed for the relevant Operational Services set out in the Transition Plan;
"Audit"	any exercise by the Authority of its Audit Rights pursuant to Clause **Error! Reference source not found.** (*Records, Reports, Audit and Open Book Data*) and Schedule 7.5 (*Financial Reports and Audit Rights)*;

"Audit Agents"	(a) the Authority's internal and external auditors; (b) the Authority's statutory or regulatory auditors; (c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; (d) HM Treasury or the Cabinet Office; (e) any party formally appointed by the Authority to carry out audit or similar review functions; and (f) successors or assigns of any of the above;
"Audit Rights"	the audit and access rights referred to in Schedule 7.5 (*Financial Reports and Audit Rights*);
"Authority Assets"	the Authority Materials, the Authority infrastructure and any other data, software, assets, equipment or other property owned by and/or licensed or leased to the Authority and which is or may be used in connection with the provision or receipt of the Services;
"Authority Background IPRs"	(a) IPRs owned by the Authority before the Effective Date, including IPRs contained in any of the Authority's Know-How, documentation, processes and procedures; (b) IPRs created by the Authority independently of this Agreement; and/or (c) Crown Copyright which is not available to the Supplier otherwise than under this Agreement; but excluding IPRs owned by the Authority subsisting in the Authority Software;
"Authority Cause"	any material breach by the Authority of any of the Authority Responsibilities, except to the extent that such breach is: (a) the result of any act or omission by the Authority to which the Supplier has given its prior consent; or (b) caused by the Supplier, any supplier or any Supplier Personnel;

"Authority Data"	(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Supplier by or on behalf of the Authority; and/or (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; (b) any Personal Data; or (c) any Sanitised Personal Data;
"Authority IT Strategy"	the Authority's IT policy in force as at the Effective Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Change Control Procedure;
"Authority Materials"	the Authority Data together with any materials, documentation, information, programs and codes supplied by the Authority to the Supplier, the IPRs in which: (a) are owned or used by or on behalf of the Authority; and (b) are or may be used in connection with the provision or receipt of the Services; but excluding any Project Specific IPRs, Specially Written Software, Supplier Software, Third-Party Software and Documentation relating to Supplier Software or Third-Party Software;
"Authority Premises"	premises owned, controlled or occupied by the Authority and/or any Central Government Body which are made available for use by the Supplier or its Sub-contractors for provision of the Services (or any of them);
"Authority Representative"	the representative appointed by the Authority pursuant to Clause **Error! Reference source not found.** (*Representatives*);
"Authority Requirements"	the requirements of the Authority set out in Schedules 2.1 (*Services Description*), 2.2 (*Performance Levels),* 2.3 (*Standards),* 2.4 (*Security Management), 2.5 (Insurance*

	Requirements), 6.1 (*Transition*), 8.2 (*Reports and Records*), 8.5 (*Exit Management*) and 8.6 (*Service Continuity Plan and Corporate Resolution Planning)*;
"Authority Responsibilities"	the responsibilities of the Authority specified in Schedule 3 (*Authority Responsibilities*);
"Authority Software"	software which is owned by or licensed to the Authority (other than under or pursuant to this Agreement) and which is or will be used by the Supplier for the purposes of providing the Services;
"Authority System"	the Authority's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Authority or the Supplier in connection with this Agreement which is owned by the Authority or licensed to it by a third party and which interfaces with the Supplier System or which is necessary for the Authority to receive the Services;
"Authority to Proceed" or "ATP"	the authorisation to the Supplier to commence the provision of the relevant Operational Services to the Authority, provided by the Authority;
"Baseline Security Requirements"	the Authority's baseline security requirements, the current copy of which is contained in Annex 1 of Schedule 2.4 (*Security Management*), as updated from time to time by the Authority and notified to the Supplier;
"Board"	means the Supplier's board of directors;
"Board Confirmation"	means the written confirmation from the Board in accordance with paragraph 8 of Schedule 7.4 (Financial Distress);
"Breakage Costs Payment"	has the meaning given in Schedule 7.2 (*Payments on Termination*);
"Business Continuity Plan"	Part B of the Service Continuity Plan, as defined in Paragraph 2.2(a)(ii) of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);
"Cabinet Office Markets and Suppliers Team"	means the UK government's team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;

"Central Government Body"	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: (a) Government Department; (b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); (c) Non-Ministerial Department; or (d) Executive Agency;
"Certificate of Costs"	has the meaning given in Schedule 7.1 (*Charges and Invoicing*);
"Change"	any change to this Agreement;
"Change Authorisation Note"	a form setting out an agreed Contract Change which shall be substantially in the form of Annex 2 of Schedule 8.3 (*Change Control Procedure*);
"Change Control Procedure"	the procedure for changing this Agreement set out in Schedule 8.3 (*Change Control Procedure*);
"Change in Law"	any change in Law which impacts on the performance of the Services which comes into force after the Effective Date;
"Change Request"	a written request for a Contract Change substantially in the form of Annex 1 of Schedule 8.3 (*Change Control Procedure);*
"Charges"	the charges for the provision of the Services set out in or otherwise calculated in accordance with Schedule 7.1 (*Charges and Invoicing)*, including any Milestone Payment or Service Charge;
"CNI"	means Critical National Infrastructure;
"Class 1 Transaction"	has the meaning set out in the listing rules issued by the UK Listing Authority;
"Commercially Sensitive Information"	the information listed in Schedule 4.2 (*Commercially Sensitive Information*) comprising the information of a commercially sensitive nature relating to; (a) the pricing of the Services;

	(b) the details of the Supplier's IPRs; and (c) the Supplier's business and investment plans; which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
"Comparable Supply"	the supply of services to another customer of the Supplier that are the same or similar to any of the Services;
"Compensation for Unacceptable Performance Failure"	has the meaning given in Clause **Error! Reference source not found.** (*Unacceptable Performance Failure*);
"Concealed IPR"	means IPR of the Supplier (or licensed to the Supplier) which is or will be used before or during the Term for designing, testing implementing and/or providing the Services which IPR is not set out in Schedule 5 (*Intellectual Property Rights*);
"Condition Precedent"	has the meaning given in Clause **Error! Reference source not found.** (*Condition Precedent*);
"Confidential Information"	a) Information, including all Personal Data, which (however it is conveyed) is provided by the Disclosing Party pursuant to or in anticipation of this Agreement that relates to: (i) the Disclosing Party Group; or (ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Disclosing Party Group; (b) other Information provided by the Disclosing Party pursuant to or in anticipation of this Agreement that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential (whether or not it is so marked) which comes (or has come) to the Recipient's attention or into the Recipient's possession in connection with this Agreement; (c) discussions, negotiations, and correspondence between the Disclosing Party or any of its directors, officers, employees, consultants or professional advisers and the Recipient or any of

its directors, officers, employees, consultants and professional advisers in connection with this Agreement and all matters arising therefrom; and

(d) Information derived from any of the above,
but not including any Information which:

(i) was in the possession of the Recipient without obligation of confidentiality prior to its disclosure by the Disclosing Party;

(ii) the Recipient obtained on a non-confidential basis from a third party who is not, to the Recipient's knowledge or belief, bound by a confidentiality agreement with the Disclosing Party or otherwise prohibited from disclosing the information to the Recipient;

(iii) was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Agreement or breach of a duty of confidentiality;

(iv) was independently developed without access to the Confidential Information; or

(v) relates to the Supplier's:

1. performance under this Agreement; or
2. failure to pay any Sub-contractor as required pursuant to Clause 15.20 (*Supply Chain Protection*);

"Connected Company" means, in relation to a company, entity or other person, the Affiliates of that company, entity or other person or any other person associated with such company, entity or other person;

"Contract Change" any change to this Agreement including IT Changes and Statement of Works. This does not include Operational Changes.

"Contracts Finder" means the online government portal which allows suppliers to search for information about contracts worth over £10,000 (excluding VAT) as prescribed by Part 4 of the Public Contracts Regulations 2015;

"Contract Inception Report"	the initial financial model in a form agreed by the Supplier and the Authority in writing on or before the Effective Date;
"Contract Year"	(a) a period of twelve (12) months commencing on the Effective Date; or (b) thereafter a period of twelve (12) months commencing on each anniversary of the Effective Date; provided that the final Contract Year shall end on the expiry or termination of the Term;
"Control"	the possession by person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "**Controls"** and "**Controlled"** shall be interpreted accordingly;
"Controller"	has the meaning given in the Relevant Data Protection Laws;
"Corporate Change Event"	means: (a) any change of Control of the Supplier or a Parent Undertaking of the Supplier; (b) any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Authority, could have a material adverse effect on the Services; (c) any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Authority, could have a material adverse effect on the Services; (d) a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc; (e) an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier;

	(f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12-month period; (g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group; (h) any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group; (i) the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or (j) any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales;
"Corporate Resolution Planning Information"	means, together, the: a) Group Structure Information and Resolution Commentary; and b) UK Public Sector and CNI Contract Information;
"Costs"	has the meaning given in Schedule 7.1 (*Charges and Invoicing*);
"CPP Milestone"	a contract performance point as set out in the Transition Plan, being the Milestone at which the Supplier has demonstrated that the Supplier Solution or relevant Service is working satisfactorily in its operating environment in accordance with Schedule 6.2 (*Testing Procedures*);

"Critical National Infrastructure"	means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or b) significant impact on national security, national defence, or the functioning of the UK;
"Critical Failure Performance Threshold"	means the relevant level of performance designated as such for a Performance Indicator and set out in the relevant table in Part I of Annex 1 of Schedule 2.2 (*Performance Levels*);
"Critical KPI Failure"	shall have the meaning given, in relation to the relevant Key Performance Indicator, in Paragraph 1.9 of Part A of Schedule 2.2 (*Performance Levels*);
"Critical Service Contract"	means the overall status of this Agreement as determined by the Authority and specified in paragraph 10.1 of Part 2 to Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);
"Crown"	means the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"Crown Copyright"	has the meaning given in the Copyright, Designs and Patents Act 1988;
"CRP Information"	means the Corporate Resolution Planning Information;
"CRTPA"	the Contracts (Rights of Third Parties) Act 1999;
"Data Protection Impact Assessment"	means an assessment by the Controller of the impact of the processing on the protection of Personal Data;

"Data Protection Officer"	has the meaning given in the Relevant Data Protection Laws;
"Data Subject"	has the meaning given in the Relevant Data Protection Laws;
"Data Subject Access Request" or "Data Subject Request"	a request made by a Data Subject in accordance with rights granted pursuant to the Relevant Data Protection Laws to access his or her Personal Data;
"Deductions"	all Service Credits, Compensation for Unacceptable Performance Failure, Delay Payments or any other deduction which is paid or payable to the Authority under this Agreement;
"Default"	any breach of the obligations of the relevant Party (including abandonment of this Agreement in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement: (a) in the case of the Authority, of its employees, servants, agents; or (b) in the case of the Supplier, of its Sub-contractors or any Supplier Personnel, in connection with or in relation to the subject-matter of this Agreement and in respect of which such Party is liable to the other;
"Defect"	(a) any error, damage or defect in the manufacturing of a Deliverable; or (b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or (c) any failure of any Deliverable to provide the performance, features and functionality specified in the Authority Requirements or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from meeting its associated Test Success Criteria; or (d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the Authority Requirements or the

	Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from meeting its associated Test Success Criteria;
"Delay"	(a) a delay in the Achievement of a Milestone by its Milestone Date; or (b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Transition Plan or Test Plan;
"Delay Deduction Period"	the period of one hundred (100) days commencing on the relevant Milestone Date;
"Delay Payments"	the amounts payable by the Supplier to the Authority in respect of a Delay in Achieving a Key Milestone as specified in Schedule 7.1 (*Charges and Invoicing*);
"Deliverable"	an item or feature delivered or to be delivered by the Supplier at or before a Milestone Date or at any other stage during the performance of this Agreement;
"Delivery Group"	has the meaning given in Schedule 2.2 (*Performance Levels*);
"Detailed Transition Plan"	the plan developed and revised from time to time in accordance with Paragraphs 3 and 4 of Schedule 6.1 (*Transition*);
"Dependent Parent Undertaking"	means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into this Agreement, including for the avoidance of doubt the provision of the Services in accordance with the terms of this Agreement;
"Disaster Recovery Plan"	The Disaster Recovery Plan shall be designed so as to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Authority supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

"Disclosing Party"	has the meaning given in Clause **Error! Reference source not found.** (*Confidentiality*);
"Disclosing Party Group"	(a) where the Disclosing Party is the Supplier, the Supplier and any Affiliates of the Supplier; and (b) where the Disclosing Party is the Authority, the Authority and any Central Government Body with which the Authority or the Supplier interacts in connection with this Agreement;
"Discovery Period"	the first phase of the service design and delivery process;
"Dispute"	any dispute, difference or question of interpretation arising out of or in connection with this Agreement, including any dispute, difference or question of interpretation relating to the Services, failure to agree in accordance with the Change Control Procedure or any matter where this Agreement directs the Parties to resolve an issue by reference to the Dispute Resolution Procedure;
"Dispute Notice"	a written notice served by one Party on the other stating that the Party serving the notice believes that there is a Dispute;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in Schedule 8.4 (*Dispute Resolution Procedure*);
"Documentation"	descriptions of the Services and Performance Indicators, details of the Supplier System (including (i) vendors and versions for off-the-shelf components and (ii) source code and build information for proprietary components), relevant design and development information, technical specifications of all functionality including those not included in standard manuals (such as those that modify system performance and access levels), configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation as: (a) is required to be supplied by the Supplier to the Authority under this Agreement; (b) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Authority to develop, configure, build, deploy, run, maintain, upgrade

	and test the individual systems that provide Services; (c) is required by the Supplier in order to provide the Services; and/or (d) has been or shall be generated for the purpose of providing the Services;
"DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes or those who use them to tell HMRC of any notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to national insurance contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868) made under section 132A of the Social Security Administration Act 1992 and in Schedule 11A to the Value Added Tax Act 1994 (as amended by Schedule 1 to the Finance (no. 2) Act 2005;
"Due Diligence Information"	any information supplied to the Supplier by or on behalf of the Authority prior to the Effective Date;
"Ecosystem Agreement"	means a contract between the Authority and one of the Ecosystem Suppliers;
"Ecosystem Dispute"	means a Multi-Collaborating Parties Dispute as defined in Annex 4 (*Dispute Resolution*) to Schedule 11 (*Collaboration*);
"Ecosystem Dispute Resolution Procedure"	means the multi-party dispute resolution procedure set out in paragraph 3 of Annex 4 (*Dispute Resolution Procedure*) to Schedule 11 (*Collaboration*);
"Ecosystem Failure"	a failure by an Other Ecosystem Supplier to perform its obligations under its Ecosystem Agreement;
"Ecosystem Supplier"	means any supplier to the Authority (including the Supplier) which: (a) has entered into an agreement incorporating:

(i) a schedule that is identical or substantially similar to Schedule 11 (*Collaboration*); and

(ii) Clauses that are identical or substantially similar to Clauses **Error! Reference source not found.** to **Error! Reference source not found.** (*Ecosystem Failures*); and

(b) is notified to the Supplier from time to time;

"EEA"	means The European Economic Area;
"Effective Date"	the later of: (a) the date on which this Agreement is signed by both Parties; and (b) the date on which the Condition Precedent has been satisfied or waived in accordance with Clause **Error! Reference source not found.** (Condition Precedent);
"EIRs"	the Environmental Information Regulations 2004, together with any guidance and/or codes of practice issued by the Information Commissioner or any Central Government Body in relation to such Regulations;
"Emergency Maintenance"	ad hoc and unplanned maintenance provided by the Supplier where: (a) the Authority reasonably suspects that the IT Environment or the Services, or any part of the IT Environment or the Services, has or may have developed a fault, and notifies the Supplier of the same; or (b) the Supplier reasonably suspects that the IT Environment or the Services, or any part the IT Environment or the Services, has or may have developed a fault;
"Employee Liabilities"	all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a

	claim or investigation related to employment including in relation to the following: (a) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments; (b) unfair, wrongful or constructive dismissal compensation; (c) compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay; (d) compensation for less favourable treatment of part-time workers or fixed term employees; (e) outstanding employment debts and unlawful deduction of wages including any PAYE and national insurance contributions; (f) employment claims whether in tort, contract or statute or otherwise; (g) any investigation relating to employment matters by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation;
"Employment Regulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the Acquired Rights Directive;
"Escalation Meeting"	shall have the meaning at clause **Error! Reference source not found.**;
"Escalation Notice"	shall have the meaning at clause **Error! Reference source not found.**;
"Escalation Process Failure"	shall have the meaning at clause **Error! Reference source not found.**;
"Escalation Process Trigger Event"	shall mean: (A) an Intervention Trigger Event; (B) Rectification Plan Failure; and/or (C) A Remedial Adviser Failure;

"Escrow Trigger Event"	shall have the meaning given at Clause 17.19 (*Escrow*);
"Estimated Year 1 Charges"	the estimated Charges payable by the Authority during the first Contract Year, as set out in the Financial Model;
"Estimated Initial Service Charges"	the estimated Service Charges payable by the Authority during the period of twelve (12) months from the first Operational Service Commencement Date, as set out in the Financial Model;
"EU"	means the European Union;
"Euro Compliant"	means that: (i) the introduction of the euro within any part(s) of the UK shall not affect the performance or functionality of any relevant items nor cause such items to malfunction, end abruptly, provide invalid results or adversely affect the Authority's business; (ii) all currency-reliant and currency-related functions (including all calculations concerning financial data) of any relevant items enable the introduction and operation of the euro; and (iii) in particular each and every relevant item shall, to the extent it performs or relies upon currency-related functions (including all calculations concerning financial data): (a) be able to perform all such functions in any number of currencies and/or in euros; (b) during any transition phase applicable to the relevant part(s) of the UK, be able to deal with multiple currencies and, in relation to the euro and the national currency of the relevant part(s) of the UK, dual denominations; (c) recognise accept, display and print all the euro currency symbols and alphanumeric codes which may be adopted by any government and other European Union body in relation to the euro; (d) incorporate protocols for dealing with rounding and currency conversion; (e) recognise data irrespective of the currency in which it is expressed (which includes the euro) and express any output data in the national currency of the relevant part(s) of the UK and/or the euro; and

	(f) permit the input of data in euro and display an outcome in euro where such data, supporting the Authority's normal business practices, operates in euro and/or the national currency of the relevant part(s) of the UK;
"Exit Management"	services, activities, processes and procedures to ensure a smooth and orderly transition of all or part of the Services from the Supplier to the Authority and/or a Replacement Supplier, as set out or referred to in Schedule 8.5 (*Exit Management*);
"Exit Plan"	the plan produced and updated by the Supplier during the Term in accordance with Paragraph 4 of Schedule 8.5 (*Exit Management*);
"Expedited Dispute Timetable"	the reduced timetable for the resolution of Disputes set out in Paragraph 3 of Schedule 8.4 (*Dispute Resolution Procedure*);
"Expert"	has the meaning given in Schedule 8.4 (*Dispute Resolution Procedure*);
"Expert Determination"	the process described in Paragraph 6 of Schedule 8.4 (*Dispute Resolution Procedure*);
"Extension Period"	has the meaning given in Clause **Error! Reference source not found.**;
"Final Termination Warning Notice"	has the meaning given to it in Clause **Error! Reference source not found.**;
"Financial Distress Event"	the occurrence of one or more of the events listed in Paragraph 3.1 of Schedule 7.4 (*Financial Distress*);
"Financial Distress Remediation Plan"	a plan setting out how the Supplier will ensure the continued performance and delivery of the Services in accordance with this Agreement in the event that a Financial Distress Event occurs;
"Financial Model"	has the meaning given in Schedule 7.5 (*Financial Reports and Audit Rights)*;
"Financial Reports"	has the meaning given in Schedule 7.5 (*Financial Reports and Audit Rights)*;
"Financial Transparency Objectives"	has the meaning given in Schedule 7.5 (*Financial Reports and Audit Rights)*;

"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time, together with any guidance and/or codes of practice issued by the Information Commissioner or any relevant Central Government Body in relation to such Act;
"Force Majeure Event"	any event outside the reasonable control of either Party affecting its performance of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including riots, war or armed conflict, acts of terrorism, acts of government, local government or regulatory bodies, fire, flood, storm or earthquake, or other natural disaster but excluding any industrial dispute relating to the Supplier or the Supplier Personnel or any other failure in the Supplier's or a Sub-contractor's supply chain;
"Force Majeure Notice"	a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;
"Former Supplier"	has the meaning given in Schedule 9.1 (*Staff Transfer*);
"General Anti -Abuse Rule"	(a) the legislation in Part 5 of the Finance Act 2013; (b) the legislation in sections 10 and 11 of the National Insurance Contributions Act 2014; and (c) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid any Tax;
"General Change in Law"	a Change in Law where the change is of a general legislative nature (including Tax or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"Good Industry Practice"	at any time the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of services similar to the Services to a customer like the Authority, such supplier seeking to comply with its

	contractual obligations in full and complying with applicable Laws;
"Goods"	has the meaning given in Clause **Error! Reference source not found.** (*Supply of Goods*);
"Group Structure Information and Resolution Commentary"	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 11 to 13 and Appendix 1 of Part 2 of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);
"Guarantee"	the deed of guarantee in favour of the Authority entered into by the Guarantor on or about the date of this Agreement (which is in the form set out in Schedule 10 (*Guarantee*)), or any guarantee acceptable to the Authority that replaces it from time to time;
"Guarantor"	Meaning given in Paragraph 1.2 (a) of Schedule 10 (*Guarantee*)
"Halifax Abuse Principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
"Health and Safety Policy"	the health and safety policy of the Authority and/or other relevant Central Government Body as provided to the Supplier on or before the Effective Date and as subsequently provided to the Supplier from time to time except any provision of any such subsequently provided policy that cannot be reasonably reconciled to ensuring compliance with applicable Law regarding health and safety;
"HMRC"	His Majesty's Revenue & Customs;
"Impact Assessment"	has the meaning given in Schedule 8.3 (*Change Control Procedure);*
"Incumbent Supplier"	means the supplier to the Authority of services similar to the Services prior to the Services Commencement Date;
"Indemnified Person"	the Authority and each and every person to whom the Authority (or any direct or indirect sub-licensee of the Authority) sub-licenses, assigns or novates any Relevant IPRs or rights in Relevant IPRs in accordance with this Agreement;

"In-Flight Projects"	the projects listed in Schedule 6.4 (*In-Flight Projects*) as amended from time to time;
"Information"	all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form);
"Initial Term"	the period of five (5) years from and including the first Operational Service Commencement Date;
"Initial Upload Date"	means the occurrence of an event detailed in Schedule 8.2 (*Reports and Records*) Annex 4 (*Records to Upload to Virtual Library*) which requires the Supplier to provide its initial upload of the relevant information to the Virtual Library;
"Insolvency Event"	with respect to any person, means: (a) that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or: (i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or (ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986; (b) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to the Insolvency Act 1986, as amended by the Corporate Insolvency and Governance Act 2020, other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that that person with one or more other companies or the solvent reconstruction of that person; (c) another person becomes entitled to appoint a receiver over the assets of that person or

a receiver is appointed over the assets of that person;

(d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person's assets and such attachment or process is not discharged within fourteen (14) days;

(e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;

(f) where that person is a company, a LLP or a partnership:

(i) a petition is presented (which is not dismissed within fourteen (14) days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;

(ii) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at Court or given or if an administrator is appointed, over that person;

(iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or

(iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or

(g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above;

"Intellectual Property Rights" or **"IPRs"** (a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions,

	semi-conductor topography rights, trade marks, rights in Internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information; (b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and (c) all other rights having equivalent or similar effect in any country or jurisdiction;
"Intervention Cause"	has the meaning given in Clause **Error! Reference source not found.** (Remedial Adviser);
"Intervention Notice"	has the meaning given in Clause **Error! Reference source not found.** (*Remedial Adviser*);
"Intervention Period"	has the meaning given in Clause **Error! Reference source not found.** (*Remedial Adviser*);
"Intervention Trigger Event"	(a) any event falling within limb (a), (c), (d), (f), (h) or (i) of the definition of a Supplier Termination Event; (b) any event falling within limb (b) or (e) of the definition of Step-In Trigger Event; (c) a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any material part of the Services; (d) the Supplier committing a Major KPI Failure or a Critical KPI Failure; and/or (e) the Supplier not Achieving a Key Milestone within seventy five (75) days of its relevant Milestone Date;
"IPRs Claim"	any claim against any Indemnified Person of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any Relevant IPRs save for any such claim to the extent that it is caused by any use by or on behalf of that Indemnified Person of any Relevant IPRs, or the use of the Authority Software by or on behalf of the Supplier, in either case in combination with any item not supplied or recommended by the Supplier pursuant to this Agreement or for a purpose

	not reasonably to be inferred from the Services Description or the provisions of this Agreement;
"IT"	information and communications technology;
"IT Change"	any change to either: integration infrastructure, data formats including print files, document composition, production capabilities, testing and/or go live processes;
"IT Environment"	the Authority System and the Supplier System;
"Key Milestone"	the Milestones identified in the Transition Plan or any Test Plan as key milestones and in respect of which Delay Payments may be payable in accordance with Paragraph 1 of Part C of Schedule 7.1 (*Charges and Invoicing*) if the Supplier fails to Achieve the Milestone Date in respect of such Milestone;
"Key Performance Indicator" or "KPI"	the key performance indicators set out in Table 1 of Part I of Annex 1 of Schedule 2.2 (*Performance Levels*);
"Key Personnel"	those persons appointed by the Supplier to fulfil the Key Roles, being the persons listed in Schedule 9.2 (*Key Personnel*) against each Key Role as at the Effective Date or as amended from time to time in accordance with Clauses **Error! Reference source not found.** and **Error! Reference source not found.** (*Key Personnel*);
"Key Roles"	a role described as a Key Role in Schedule 9.2 (*Key Personnel*) and any additional roles added from time to time in accordance with Clause **Error! Reference source not found.** (*Key Personnel*);
"Key Sub-contract"	each Sub-contract with a Key Sub-contractor;
"Key Sub-contractor"	any Sub-contractor: (a) which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or (b) with a Sub-contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) ten per cent (10%) of the aggregate Charges forecast to be

	payable under this Agreement (as set out in the Financial Model);
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the Services but excluding know how already in the other Party's possession before this Agreement;
"KPI Failure"	a failure to meet the Target Performance Level in respect of a Key Performance Indicator;
"Law"	any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply;
"Licensed Software"	all and any Software licensed by or through the Supplier, its Sub-contractors or any third party to the Authority for the purposes of or pursuant to this Agreement, including any Supplier Software, Third-Party Software and/or any Specially Written Software;
"LLP"	means Limited Liability Partnership, as defined in s.1(2) of the Limited Liability Partnerships Act 2000;
"Losses"	losses, liabilities, damages, costs and expenses (including legal fees on a solicitor/client basis) and disbursements and costs of investigation, litigation, settlement, judgment interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty or otherwise;
"Maintenance Schedule"	shall have the meaning set out in Clause **Error! Reference source not found.** (*Maintenance*);
"Major Failure Performance Threshold"	means the relevant level of performance designated as such for a Performance Indicator and set out in the relevant table in Part I of Annex 1 of Schedule 2.2 (Performance Levels);
"Major KPI Failure"	shall have the meaning given, in relation to the relevant Key Performance Indicator, in paragraph 1.7 of Part A of Schedule 2.2 (*Performance Levels*);

"Major SPI Failure"	shall have the meaning given, in relation to the relevant Subsidiary Performance Indicator, in paragraph 1.7 of Part A of Schedule 2.2 (Performance Levels);
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"Management Information" or "MI"	the management information specified in Schedule 2.2 (*Performance Levels*), Schedule 7.1 (*Charges and Invoicing*) and Schedule 8.1 (*Governance*) to be provided by the Supplier to the Authority;
"Measurement Period"	in relation to a Key Performance Indicator or Subsidiary Performance Indicator, the period over which the Supplier's performance is measured (for example, a Service Period if measured monthly or a twelve (12) month period if measured annually), as is specified for each Key Performance Indicator and Subsidiary Performance Indicator in the relevant table set out at Annex 1 to Schedule 2.2 (*Performance Levels*);
"Milestone"	an event or task described in the Transition Plan which, if applicable, shall be completed by the relevant Milestone Date;
"Milestone Adjustment Payment Amount"	in respect of each CPP Milestone the subject of a Milestone Adjustment Payment Notice, an amount determined in accordance with the formula: A – B where: (a) A is an amount equal to the aggregate sum of all Milestone Payments paid to the Supplier in respect of the Milestones (or in the case of Partial Termination, the Milestones for the parts of the Services terminated) relating to that CPP Milestone; and (b) B is an amount equal to the aggregate Allowable Price for the Retained Deliverables

	relating to that CPP Milestone or, if there are no such Retained Deliverables, zero;
"Milestone Adjustment Payment Notice"	has the meaning given in Clause **Error! Reference source not found.** (*Payments by the Supplier*);
"Milestone Date"	the target date set out against the relevant Milestone in the Transition Plan or a Testing Plan by which the Milestone must be Achieved;
"Milestone Payment"	a payment identified in Schedule 7.1 (*Charges and Invoicing*)
"Milestone Retention"	has the meaning given in Schedule 7.1 (*Charges and Invoicing);*
"Minor KPI Failure"	shall have the meaning given, in relation to the relevant Key Performance Indicator, in Paragraph 1.9 of Part A of Schedule 2.2 (*Performance Levels*);
"Minor SPI Failure"	shall have the meaning given, in relation to the relevant Subsidiary Performance Indicator, in Paragraph 1.9 of Part A of Schedule 2.2 (*Performance Levels*);
"Month"	a calendar month and **"monthly"** shall be interpreted accordingly;
"Related Third-Party Dispute Initiation Notice"	has the meaning given in Paragraph 9.2 of Schedule 8.4 (*Dispute Resolution Procedure*);
"Related Third-Party Dispute Resolution Procedure"	has the meaning given in Paragraph 9.1 of Schedule 8.4 (*Dispute Resolution Procedure*);
"New Releases"	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
"Non-Party IPRs"	any Intellectual Property Right owned or claimed to be owned by any third party which is found, or alleged to be found, in the Specially Written Software and the Project Specific IPRs;
"Non-retained Deliverables"	in relation to a CPP Milestone Payment Notice and each CPP Milestone the subject of that CPP

	Milestone Payment Notice, Deliverables provided to the Authority which relate to the relevant CPP Milestone(s) and which are not Retained Deliverables;
"Non-trivial Customer Base"	a significant customer base with respect to the date of first release and the relevant market but excluding Affiliates and other entities related to the licensor;
"Notifiable Default"	shall have the meaning given in Clause 27.2 (*Rectification Plan Process*);
"Object Code"	software and/or data in machine-readable, compiled object code form;
"Occasion of Tax Non-Compliance"	where an entity or person under consideration meets all 3 conditions contained in the relevant excerpt from HMRC's "Test for Tax Non-Compliance", as set out in Annex 1 of this Schedule, where: (a) the "Economic Operator" means the Supplier or any agent, supplier or Subcontractor of the Supplier requested to be replaced pursuant to Clause 4.3; and (b) any "Essential Subcontractor" means any Key Subcontractor;
"Off-shore Location"	any place outside of the United Kingdom;
"Open Book Data"	has the meaning given in Schedule 7.5 (*Financial Reports and Audit Rights*)
"Open Source"	software that is released on the internet for use by any person, such release usually being made under a recognised open source licence and stating that it is released as open source;
"Open Source Publication Material"	has the meaning given in Clause **Error! Reference source not found.**A.2(f);
"Operating Environment"	the Authority System and the Sites;
"Operational Change"	any change in the Supplier's operational procedures which in all respects, when implemented: (a) will not affect the Charges and will not result in any other costs to the Authority;

	(b) may change the way in which the Services are delivered but will not adversely affect the output of the Services or increase the risks in performing or receiving the Services; (c) will not adversely affect the interfaces or interoperability of the Services with any of the Authority's IT infrastructure; and (d) will not require a change to this Agreement;
"Operational Service Commencement Date"	in relation to an Operational Service, where the Transition Plan states that the Supplier must have Achieved the relevant ATP Milestone before it can commence the provision of that Operational Service, the date upon which the Supplier Achieves the relevant ATP Milestone;
"Operational Services"	the operational services described as such in the Services Description;
"Other Ecosystem Model"	the overarching term for the scope of the operating model comprised of the Authority and the Other Ecosystem Suppliers;
"Other Ecosystem Supplier(s)"	the Ecosystem Supplier(s) excluding the Supplier;
"Other Ecosystem Supplier Delay"	(a) a delay by an Other Ecosystem Supplier to achieve a milestone by its milestone date in accordance with its Ecosystem Agreement; or (b) a delay by an Other Ecosystem Supplier to design, develop, test or implement a deliverable by the relevant date set out in that Ecosystem Supplier's transition plan or any;
"Other Supplier"	any other third party which supplies services to the Authority, including the Other Ecosystem Suppliers but excluding the Incumbent Suppliers;
"Overhead"	those amounts which are intended to recover a proportion of the Supplier's or the Key Sub-contractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Personnel and accordingly included within limb (a) of the definition of "Costs" or the day cost set out in Table **Error! Reference source not found.**

	of Annex **Error! Reference source not found.** of Schedule 7.1 (*Charges and Invoicing*);
"Parent Undertaking"	has the meaning set out in section 1162 of the Companies Act 2006;
"Partial Termination"	the partial termination of this Agreement to the extent that it relates to the provision of any part of the Services as further provided for in Clause **Error! Reference source not found.** (*Termination by the Authority*) or **Error! Reference source not found.** (*Termination by the Supplier*), or otherwise by mutual agreement by the Parties;
"Parties" and **"Party"**	have the meanings respectively given in Clauses 1.3 - 1.6 of this Agreement;
"Performance Failure"	a KPI Failure or an SPI Failure;
"Performance Indicators"	the Key Performance Indicators and the Subsidiary Performance Indicators;
"Performance Monitoring Report"	has the meaning given in Schedule 2.2 (*Performance Levels*);
"Permitted Maintenance"	has the meaning given in Clause **Error! Reference source not found.** (*Maintenance*);
"Persistent Breach"	means a Default which continued or recurred on more than one occasion within a six (6) month period following the date of a Final Termination Warning Notice;
"Personal Data"	personal data (as defined in the Relevant Data Protection Laws) which is Processed by the Supplier or any Sub-contractor pursuant to or in connection with this Agreement;
"Personal Data Breach"	means: (a) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed; (b) a discovery or reasonable suspicion that there is a vulnerability in any technological measure used to protect any Personal Data that has previously been subject to a breach within the scope of paragraph

	(a), which may result in exploitation or exposure of that Personal Data; or (c) any defect or vulnerability with the potential to impact the ongoing resilience, security and/or integrity of systems Processing Personal Data;
"Preceding Services"	has the meaning given in Clause **Error! Reference source not found.** (*Standard of Services)*;
"Process"	has the meaning given to it under the Relevant Data Protection Laws and "**Processed**" and "**Processing**" shall be construed accordingly;
"Processor"	has the meaning given in the Relevant Data Protection Laws;
"Prohibited Act"	(a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority a financial or other advantage to: (i) induce that person to perform improperly a relevant function or activity; or (ii) reward that person for improper performance of a relevant function or activity; (b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this Agreement; (c) an offence: (i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); (ii) under legislation or common law concerning fraudulent acts (including offences by the Supplier under Part 3 of the Criminal Finances Act 2017); or (iii) defrauding, attempting to defraud or conspiring to defraud the Authority; or (d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;

"Prohibited Transaction"	has the meaning given in Clause **Error! Reference source not found.** (*Use of Off-shore Tax Structures*);
"Project Specific IPRs"	(a) Intellectual Property Rights in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Agreement and updates and amendments of these items including (but not limited to) database schema; and/or (b) Intellectual Property Rights arising as a result of the performance of the Supplier's obligations under this Agreement; but shall not include the Supplier Background IPRs or the Specially Written Software;
"Public Sector Dependent Supplier"	means a supplier where that Supplier, or that Supplier's Group has Annual Revenue of £50 million or more of which over 50% is generated from UK Public Sector Business;
"Public Sector and CNI Contract Information"	means the information requirements set out in accordance with Paragraphs 11 to 13 and Appendix II of Part 2 of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);
"Publishable Performance Information"	means any of the information in the Performance Monitoring Report as it relates to a Performance Indicator where it is expressed as publishable in the table in Annex 1 of Schedule 2.2 which shall not constitute Commercially Sensitive Information;
"Quality Plans"	has the meaning given in Clause **Error! Reference source not found.** (*Quality Plans*);
"Quarter"	the first three Service Periods and each subsequent three (3) Service Periods (save that the final Quarter shall end on the date of termination or expiry of this Agreement);
"Recipient"	has the meaning given in Clause **Error! Reference source not found.** (*Confidentiality*);
"Records"	has the meaning given in Schedule 8.2 (*Reports and Records*);
"Rectification Plan"	a plan to address the impact of, and prevent the reoccurrence of, a Notifiable Default;

"Rectification Plan Failure"

(a) the Supplier failing to submit or resubmit a draft Rectification Plan to the Authority within the timescales specified in Clauses 27.5 (*Submission of the draft Rectification Plan*) and/or 27.9 (*Agreement of the Rectification Plan*);

(b) the Authority, acting reasonably, rejecting a revised draft of the Rectification Plan submitted by the Supplier pursuant to Clause 27.8 (*Agreement of the Rectification Plan*);

(c) the Supplier failing to rectify a material Default within the later of:

(i) thirty (30) Working Days of a notification made pursuant to Clause 27.3 (*Notification);* and

(ii) where the Parties have agreed a Rectification Plan in respect of that material Default and the Supplier can demonstrate that it is implementing the Rectification Plan in good faith, the date specified in the Rectification Plan by which the Supplier must rectify the material Default;

(d) where a Rectification Plan has been implemented, a Performance Failure re-occurring in respect of the same Key Performance Indicator and for the same (or substantially the same) root cause (in relation to which a Rectification Plan was implemented) on two or more occasions in the period ending on the date falling 6 months (or, where the relevant KPI has a Measurement Period longer than 6 months, at the end of the next complete Measurement Period) following the date set for the completion of the Rectification Plan (or, if later, the date that the Supplier indicates that the Rectification Plan is complete);

(e) the Supplier not Achieving a Key Milestone by the expiry of the Delay Deduction Period; and/or

(f) following the successful implementation of a Rectification Plan, the same Notifiable Default

	recurring within a period of six (6) months for the same (or substantially the same) root cause as that of the original Notifiable Default;
"Rectification Plan Process"	the process set out in Clauses 27.5 (*Submission of the Rectification Plan*) to 27.10 (*Agreement of the Rectification Plan*);
"Registers"	has the meaning given in Schedule 8.5 (*Exit Management*);
"Reimbursable Expenses"	has the meaning given in Schedule 7.1 (*Charges and Invoicing*);
"Relevant Authority" or "Relevant Authorities"	means the Authority and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;
"Release"	means in relation to any Deliverables (including Specially Written Software and Project Specific IPRs (which are in the nature of software)) the stage in the development process whereby those Deliverables are intended to be put in to live operation or production following successful completion of acceptance tests;
"Relevant Data Protection Laws"	means: (i) the Data Protection Act 2018; (ii) the UK GDPR, the Law Enforcement Directive (Directive EU 2016/680) and any applicable national implementing Laws as amended from time to time; (iii) any other applicable Laws relating to the processing of personal data and privacy; and (iv) all applicable guidance, standard terms, codes of practice and codes of conduct issued by the Information Commissioner and other relevant regulatory, supervisory and legislative bodies in relation to such Laws;
"Relevant IPRs"	IPRs used to provide the Services or as otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Authority or a third party in the fulfilment of the Supplier's obligations under this Agreement including IPRs in the Specially Written Software, the Supplier Non-COTS Software, the Supplier Non-COTS Background IPRs, the Third-Party Non-COTS Software and the Third-Party Non-COTS IPRs but excluding any IPRs in the Authority Software, the

	Authority Background IPRs, the Supplier COTS Software, the Supplier COTS Background IPRS, the Third-Party COTS Software and/or the Third-Party COTS IPRs;
"Relevant Preceding Services"	has the meaning given in Clause 5.1(b)(ii) (*Standard of Services*);
"Relevant Requirements"	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010;
"Relevant Tax Authority"	HMRC, or, if applicable, a tax authority in the jurisdiction in which the Supplier is established, resident or liable to any Tax;
"Relevant Transfer"	a transfer of employment to which the Employment Regulations applies;
"Relief Notice"	has the meaning given in Clause **Error! Reference source not found.** (*Authority* Cause and Ecosystem Failures);
"Remedial Adviser"	the person appointed pursuant to Clause **Error! Reference source not found.** (*Remedial Adviser*);
"Remedial Adviser Failure"	has the meaning given in Clause 30.7 (*Remedial Adviser*);
"Replacement Services"	any services which are the same as or substantially similar to any of the Services and which the Authority receives in substitution for any of the Services following the expiry or termination or Partial Termination of this Agreement, whether those services are provided by the Authority internally and/or by any third party;
"Replacement Supplier"	any third-party service provider of Replacement Services appointed by the Authority from time to time (or where the Authority is providing replacement Services for its own account, the Authority);
"Request For Information"	a Request for Information under the FOIA or the EIRs;

"Required Action"	has the meaning given in Clause **Error! Reference source not found.** (*Step-In Rights*);
"Retained Deliverables"	has the meaning given in Clause **Error! Reference source not found.** (*Payments by the Supplier*);
"Risk Register"	the register of risks and contingencies that have been factored into any Costs due under this Agreement, a copy of which is set out in Annex 4 of Schedule 7.1 (*Charges and Invoicing*);
"Sanitised Personal Data"	data derived from Authority Personal Data which has had any designatory data identifiers removed so that an individual cannot be identified;
"Security Management Plan"	the Supplier's security plan as attached as Annex 2 of Schedule 2.4 (*Security Management*) and as subsequently developed and revised pursuant to Paragraphs 4 and 5 of Schedule 2.4 (*Security Management*);
"Service Beneficiary"	means an entity, other than the Authority, that may receive the benefit of some aspect of the Services and whom the Authority shall notify to the Supplier from time to time (an indicative and non-exhaustive list of Services Beneficiaries is set out in Schedule 2.7 (*Services Recipients and Services Beneficiaries*);
"Service Charge(s)"	the periodic payments made by the Supplier to the Authority in accordance with Schedule 7.1 (*Charges and Invoicing*) and as referred to in Schedule 2.2 (*Performance Levels*), in respect of the supply of the Operational Services;
"Service Continuity Plan"	any plan prepared pursuant to Paragraph 2 of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*) as may be amended from time to time;
"Service Continuity Services"	the business continuity, disaster recovery and insolvency continuity services set out in Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);
"Service Credit Cap"	has the meaning given in paragraph 6.3 of Part A (*Performance Indicators and Service Credits*) of Schedule 2.2 (*Performance Levels*);
"Service Credits"	credits payable by the Supplier due to the occurrence

	of one (1) or more KPI Failures, calculated in accordance with Paragraph 3 Part C of Schedule 7.1 (*Charges and Invoicing*);
"Service Period"	a calendar month, save that: (a) the first service period shall begin on the first Operational Service Commencement Date and shall expire at the end of the calendar month in which the first Operational Service Commencement Date falls; and (b) the final service period shall commence on the first day of the calendar month in which the Term expires or terminates and shall end on the expiry or termination of the Term;
"Service Points"	in relation to a KPI Failure, the points that are set out against the relevant Key Performance Indicator in the table in Annex 1 of Schedule 2.2 (*Performance Levels*);
"Service Recipient"	means those listed as such in Schedule 2.7 (*Service Recipients and Service Beneficiaries*) (as such Schedule is amended from time to time by the Authority), being Other Government Departments and any other third party other than the Authority to which the Supplier shall provide all or part of the Services;
"Services"	any and all of the services to be provided by the Supplier under this Agreement, including those set out in Schedule 2.1 (*Services Description*);
"Services Description"	the services description set out in Schedule 2.1 (*Services Description*);
"Service Transfer Date"	has the meaning given in Schedule 9.1 (*Staff Transfer*);
"Sites"	any premises (including the Authority Premises, se): (a) from, to or at which: (i) the Services are (or are to be) provided; or (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where: (i) any part of the Supplier System is

situated; or

(ii) any physical interface with the Authority System takes place;

"SME"	means an enterprise falling within the category of micro, small and medium-sized enterprises defined by the European Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;
"Social Value"	means the social, economic or environmental benefits set out in the Authority's Requirements;
"Software"	Specially Written Software, Supplier Software and Third-Party Software;
"Software Supporting Materials"	has the meaning given in Clause **Error! Reference source not found.** (*Specially Written Software and Project Specific IPRs*);
"Source Code"	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
"Specially Written Software"	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-contractor or other third party on behalf of the Supplier) specifically for the purposes of this Agreement, including any modifications or enhancements to Supplier Software or Third-Party Software created specifically for the purposes of this Agreement;
"Specific Change in Law"	a Change in Law that relates specifically to the business of the Authority and which would not affect a Comparable Supply;
"SPI Failure"	a failure to meet the Target Performance Level in respect of a Subsidiary Performance Indicator;
"Staffing Information"	has the meaning given in Schedule 9.1 (*Staff Transfer*);

"Standards"	the standards, polices and/or procedures identified in Schedule 2.3 (*Standards*) and as updated from time to time by the Authority and notified to the Supplier;
"Statement of Works"	A document that provides a description of requirements and defines the scope of the work being carried out. As referred to in Schedule 2.1 (*Services Descriptions*) In the form of Annex 1.15;
"Step-In Notice"	has the meaning given in Clause **Error! Reference source not found.** *(Step-In Rights)*;
"Step-In Trigger Event"	(a) any event falling within the definition of a Supplier Termination Event; (b) a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any material part of the Services; (c) the Authority considers that the circumstances constitute an emergency despite the Supplier not being in breach of its obligations under this Agreement; (d) the Authority being advised by a regulatory body that the exercise by the Authority of its rights under Clause **Error! Reference source not found.** (Step-In Rights) is necessary; (e) the existence of a serious risk to the health or safety of persons, property or the environment in connection with the Services; and/or (f) a need by the Authority to take action to discharge a statutory duty;
"Step-Out Date"	has the meaning given in Clause **Error! Reference source not found.** (*Step-In Rights*);
"Step-Out Notice"	has the meaning given in Clause **Error! Reference source not found.** (*Step-In Rights*);
"Step-Out Plan"	has the meaning given in Clause **Error! Reference source not found.** (*Step-In Rights*);
"Strategic Supplier"	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers;

"Strategic Board"	has the meaning given in Schedule 8.1 (*Governance*);
"Sub-contract"	any contract or agreement (or proposed contract or agreement) between the Supplier (or a Sub-contractor) and any third party whereby that third party agrees to provide to the Supplier (or the Sub-contractor) all or any part of the Services or facilities or services which are material for the provision of the Services or any part thereof or necessary for the management, direction or control of the Services or any part thereof;
"Sub-contractor"	any third party with whom: (a) the Supplier enters into a Sub-contract; or (b) a third party under (a) above enters into a Sub-contract, or the servants or agents of that third party;
"Sub-processor"	has the meaning given at Clause 23.5;
"Subsidiary Undertaking"	has the meaning set out in section 1162 of the Companies Act 2006;
"Subsidiary Performance Indicator" or "SPI"	the performance indicators set out in Table 2 of Part I of Annex 1 of Schedule 2.2 (*Performance Levels*);
"Successor Body"	has the meaning given in Clause **Error! Reference source not found.** (*Assignment and Novation*);
"Supplier"	has the meaning given on page 5 of the Terms and Conditions of this Agreement.
"Supplier Background IPRs"	(a) Intellectual Property Rights owned by the Supplier before the Effective Date, for example those subsisting in the Supplier's standard development tools, program components or standard code used in computer programming or in physical or electronic media containing the Supplier's Know-How or generic business methodologies; and/or (b) Intellectual Property Rights created by the Supplier independently of this Agreement, which in each case is or will be used before or during the Term for designing, testing implementing or providing the Services but excluding Intellectual

	Property Rights owned by the Supplier subsisting in the Supplier Software;
"Supplier COTS Background IPRs"	means any embodiments of Supplier Background IPRs that: (a) the Supplier makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and (b) has a Non-trivial Customer Base;
"Supplier COTS Software"	Supplier Software (including open source software) that: (a) the Supplier makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and (b) has a Non-trivial Customer Base;
"Supplier Equipment"	the hardware, computer and telecoms devices and equipment used by the Supplier or its Sub-contractors (but not hired, leased or loaned from the Authority) for the provision of the Services;
"Supplier Executive"	means the member elected by the Supplier to manage any escalations in accordance with Clause 29 (*Escalation Process*), and named in Schedule 9.2 (*Key Personnel*);
"Supplier Group"	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
"Supplier Non-COTS Background IPRs"	any embodiments of Supplier Background IPRs that have been delivered by the Supplier to the Authority and that are not Supplier COTS Background IPRs;
"Supplier Non-COTS Software"	Supplier Software that is not Supplier COTS Software;
"Supplier Non-Performance"	has the meaning given in Clause **Error! Reference source not found.** (*Authority Cause and Ecosystem Failures*);
"**Supplier Personnel**"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Sub-

	contractor engaged in the performance of the Supplier's obligations under this Agreement;
"Supplier Profit"	has the meaning given in Schedule 7.1 (*Charges and Invoicing*);
"Supplier Profit Margin"	has the meaning given in Schedule 7.1 (*Charges and Invoicing*);
"Supplier Representative"	the representative appointed by the Supplier pursuant to Clause **Error! Reference source not found.** (*Representatives);*
"Supplier Software"	software which is proprietary to the Supplier (or an Affiliate of the Supplier) and which is or will be used by the Supplier for the purposes of providing the Services as specified as such in Schedule 5 (*IPR*) or as agreed in accordance with Clause **Error! Reference source not found.**;
"Supplier Solution"	the Supplier's solution for the Services set out in Schedule 4.1 (*Supplier Solution*) including any Annexes of that Schedule;
"Supplier System"	the information and communications technology system used by the Supplier in implementing and performing the Services including the Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Authority System);

"Supplier Termination Event"

(a) the Supplier's level of performance constituting an Unacceptable Performance Failure or a Critical KPI Failure;

(b) the Supplier's level of performance constitutes a Persistent Breach;

(c) the Supplier committing a material Default which is irremediable;

(d) as a result of the Supplier's Default, the Authority incurring Losses in any Contract Year which exceed eighty (80) per cent of the value of the aggregate annual liability cap for that Contract Year as set out in Clause **Error! Reference source not found.** (*Financial Limits*);

(e) a Remedial Adviser Failure;

(f) a Rectification Plan Failure;

(g) an Escalation Process Failure;

(h) where a right of termination is expressly reserved in this Agreement, including pursuant to:

(i) Clause **Error! Reference source not found.** (*IPRs Indemnity*);

(ii) Clause **Error! Reference source not found.** (*Prevention of Fraud and Bribery*); and/or

(iii) Paragraph 4 of Schedule 7.4 (*Financial Distress*);

(iv) Paragraph 12 of Part 2 to Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);

(i) the representation and warranty given by the Supplier pursuant to Clause **Error! Reference source not found.** (*Warranties*) being materially untrue or misleading;

(j) the Supplier committing a material Default or failing to provide details of steps being taken and mitigating factors pursuant to Clauses 10.9 to 10.17 (*Promoting Tax Compliance*) which in the reasonable opinion of the Authority are acceptable;

(k) the Supplier committing a material Default under any of the following:

(i) Clause **Error! Reference source not found.** (*Services*);

(ii) Clauses 10.09 to 10.17 (inclusive) (*Promoting Tax Compliance*);

(iii) Clauses 10.18 and 10.21 (*Use of Off-shore Tax Structures*);

(iv) Clause **Error! Reference source not found.** (*Income Tax and National Insurance Contributions*);

(v) Clause **Error! Reference source not found.** (*Protection of Personal Data);*

(vi) Clause **Error! Reference source not found.** (*Transparency and Freedom of Information*);

(vii) Clause **Error! Reference source not found.** (*Confidentiality*);

(viii) Clause **Error! Reference source not found.** (*Compliance*);

(vi) in respect of any security requirements set out in Schedule 2.1 (*Services Description*), Schedule 2.4 (*Security Management*) or the Baseline Security Requirements; and/or

(vii) in respect of any requirements set out in Schedule 9.1 (*Staff Transfer*);

(l) any failure by the Supplier to implement the changes set out in a Benchmark Report as referred to in Paragraph 5.8 of Schedule 7.3 (*Value for Money*);

(m) an Insolvency Event occurring in respect of the Supplier or the Guarantor;

(n) the Guarantee ceasing to be valid or enforceable for any reason (without the Guarantee being replaced with a comparable guarantee to the satisfaction of the Authority with the Guarantor or with another guarantor which is acceptable to the Authority);

(o) a change of Control of the Supplier or a Guarantor unless:

(i) the Authority has given its prior written consent to the particular change of Control,

which subsequently takes place as proposed; or

(ii) the Authority has not served its notice of objection within six (6) months of the later of the date on which the Change of Control took place or the date on which the Authority was given notice of the change of Control;

(p) a change of Control of a Key Sub-contractor unless, within six (6) months of being notified by the Authority that it objects to such change of Control, the Supplier terminates the relevant Key Sub-contract and replaces it with a comparable Key Sub-contract which is approved by the Authority pursuant to Clause 15.12 (*Appointment of Key Sub-contractors*);

(q) any failure by the Supplier to enter into or to comply with an Admission Agreement to either Part A or Part B of Schedule 9.1 (*Staff Transfer*);

(r) the Authority has become aware that the Supplier should have been excluded under Regulation 57(1), (2) or (3) of the Public Contracts Regulations 2015 from the procurement procedure leading to the award of this Agreement;

(s) the Supplier:

(i) commits an irremediable breach of the Admission Agreement; or

(ii) commits a breach of the Admission Agreement which, where capable of remedy, it fails to remedy within a reasonable time and in any event within 28 days of the date of a notice giving particulars of the breach and requiring the Supplier to remedy it; or

(t) a failure by the Supplier to comply in the performance of the Services with legal obligations in the fields of environmental, social or labour law;

(u) the Supplier commits a breach of any of the requirements set out at Clause 36.5 (Modern Slavery Act);

"Supply Chain Transparency Information Report"	means the report provided by the Supplier to the Authority in the form set out in Annex 5 of Schedule 8.2 (*Reports and Records*);
"TAAR" or "Targeted Anti-Avoidance Rule"	means provision(s) in any legislation which seeks to prevent avoidance of any Tax;
"Target Cost"	has the meaning given in Paragraph 4.1 of Part A of Schedule 7.1 (*Charges & Invoicing*);
"Target Performance Level"	the minimum level of performance for a Performance Indicator which is required by the Authority, as set out in respect of the relevant Performance Indicator in the tables in Annex 1 of Schedule 2.2 (*Performance Levels*);
"Tax"	means: (a) all forms of tax whether direct or indirect; (b) national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction; (c) all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions, levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and (d) any penalty, fine, surcharge, interest, charges or costs relating to any of the above, in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction;
"Tax Revenue"	means any Tax, levy or duty due to be collected by the Authority and/or any reimbursement of Tax, levy or duty, correctly paid to the Authority, as a result of a Default by the Supplier;
"Term"	the period commencing on the Effective Date and ending on the expiry of the Initial Term or any Extension Period or on earlier termination of this Agreement;
"Termination Assistance Notice"	has the meaning given in Paragraph 7.1 of Schedule 8.5 (*Exit Management*);

"Termination Assistance Period"	in relation to a Termination Assistance Notice, the period specified in the Termination Assistance Notice for which the Supplier is required to provide the Termination Services as such period may be extended pursuant to Paragraph 7.3 of Schedule 8.5 (*Exit Management*);
"Termination Date"	the date set out in a Termination Notice on which this Agreement (or a part of it as the case may be) is to terminate;
"Termination Notice"	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate this Agreement (or any part thereof) on a specified date and setting out the grounds for termination;
"Termination Payment"	the payment determined in accordance with Schedule 7.2 (*Payments on Termination*);
"Termination Services"	the services and activities to be performed by the Supplier pursuant to the Exit Plan, including those activities listed in Annex 1 of Schedule 8.5 (*Exit Management*), and any other services required pursuant to the Termination Assistance Notice;
"Termination Warning Notice"	has the meaning given to it in Clause **Error! Reference source not found.**;
"Test Issue"	has the meaning given in Schedule 6.2 (*Testing Procedures*);
"Test" and "Testing"	any tests required to be carried out under this Agreement, as further described in Schedule 6.2 (*Testing Procedures*) and "**Tested"** shall be construed; accordingly,
"Third-Party Auditor"	an independent third-party auditor as appointed by the Authority from time to time to confirm the completeness and accuracy of information uploaded to the Virtual Library in accordance with the requirements outlined in Schedule 8.2 (*Reports and Records*);
"Third-Party Beneficiary"	has the meaning given in Clause **Error! Reference source not found.** (*Third-Party Rights*);

"Third-Party Contract"	means a Sub-Contract which is entered into without the Authority's consent in accordance with clause 15.9 of the contract, the details of which are recorded in Schedule 4.4;
"Third-Party COTS IPRs"	Third-Party IPRs that: (a) the Supplier makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and (b) has a Non-trivial Customer Base;
"Third-Party COTS Software"	Third-Party Software (including open-source software) that: (a) the Supplier makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and (b) has a Non-trivial Customer base;
"Third-Party IPRs"	Intellectual Property Rights owned by a third party but excluding Intellectual Property Rights owned by the third party subsisting in any Third-Party Software as specified as such in Schedule 5 (*Intellectual Property Rights*) or as agreed in accordance with Clause 17.11;
"Third-Party Non-COTS IPRs"	Third-Party IPRs that are not Third-Party COTS IPRs;
"Third-Party Non-COTS Software"	Third-Party Software that is not Third-Party COTS Software;
"Third-Party Provisions"	has the meaning given in Clause **Error! Reference source not found.** (*Third-Party Rights*);
"Third-Party Software"	software which is proprietary to any third party (other than an Affiliate of the Supplier) or any Open Source software which in any case is, will be or is proposed to be used by the Supplier for the purposes of providing the Services, as specified as such in Schedule 5 (*Intellectual Property Rights*) or as agreed in accordance with Clause 17.11;
"Transferring Assets"	has the meaning given in Paragraph 9.2 (a) of Schedule 8.5 (*Exit Management*);

"Transferring Authority Employees"	has the meaning given in Schedule 9.1 (*Staff Transfer*);
"Transferring Former Supplier Employees"	has the meaning given in Schedule 9.1 (*Staff Transfer*);
"Transferring Supplier Employees"	has the meaning given in Schedule 9.1 (*Staff Transfer*);
"Transparency Information"	has the meaning given in Clause 22.1 (*Transparency and Freedom of Information*);
"Transparency Reports"	has the meaning given in Schedule 8.2 (*Reports and Records*);
"Transition"	has the meaning given in Schedule 6.1 (*Transition*);
"Transition Plan"	the Outline Transition Plan and the Detailed Transition Plan as described in Schedule 6.1 (*Transition*);
"UK"	the United Kingdom;
"UK GDPR"	means, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (EU GDPR) 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 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419) along with the codes of practice, codes of conduct, regulatory guidance and standard clauses and other related or equivalent domestic legislation, as updated from time to time;
"UK Public Sector Business"	means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations;

"UK Public Sector / CNI Contract Information"	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 11 to 13 and Appendix III of Part 2 of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);
"Unacceptable Performance Failure"	the Supplier committing a Performance Failure in respect of 75% or more of the Performance Indicators that are measured in a Service Period in relation to a Delivery Groups;
"Unconnected Sub-contract"	means any contract or agreement which is not a Sub-contract and is between the Supplier and a third party (which is not an Affiliate of the Supplier) and is a qualifying contract under regulation 6 of the Reporting on Payment Practices and Performance Regulations 2017;
"Unconnected Sub-contractor"	means any third party with whom the Supplier enters into an Unconnected Subcontract;
"Unrecovered Payment"	has the meaning given in Schedule 7.2 (*Payments on Termination*);
"Updates"	in relation to any Software and/or any Deliverable means a version of such item which has been produced primarily to overcome Defects in, or to improve the operation of, that item;
"Update Requirement"	means the occurrence of an event detailed in Schedule 8.2 (*Reports and Records*) Annex 4 (*Records to Upload to Virtual Library*) which requires the Supplier to update the relevant information hosted on the Virtual Library;
"Upgrade"	any patch, New Release or upgrade of Software and/or a Deliverable, including standard upgrades, product enhancements, and any modifications, but excluding any Update which the Supplier or a third-party software supplier (or any Affiliate of the Supplier or any third party) releases during the Term;
"Valid"	in respect of an Assurance, has the meaning given to it in Paragraph 11.7 of Part 2 to Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);

"VAT"	value added tax as provided for in the Value Added Tax Act 1994;
"VCSE"	means voluntary, community and social enterprises which are non-governmental organisations that are value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
"Virtual Library"	means the data repository hosted by the Supplier containing the information about this Agreement and the Services provided under it in accordance with Schedule 8.2 (*Reports and Records*);
"Working Day"	means any day other than: (a) a Saturday or a Sunday; (b) Christmas Day or Good Friday; or (c) a day which is a bank holiday in England and Wales under the Banking and Financial Dealings Act 1971.

Annex 1

Excerpt from HMRC's "Test for Tax Non-Compliance"

Condition one (An in-scope entity or person)

1. There is a person or entity ("X") which is either:

   (a) The Economic Operator or Essential Subcontractor ("EOS");
   (b) Part of the same group of companies as EOS. An entity will be treated as within the same group of EOS where that entities' financial statements would be required to be consolidated with those of EOS if prepared in accordance with *IFRS 10 Consolidated Financial Accounts*[1];
   (c) Any director, shareholder or other person ("P") which exercises control over EOS. 'Control' means P can secure, through holding of shares or powers under articles of association or other document that EOS's affairs are conducted in accordance with P's wishes.

Condition two (Arrangements involving evasion, abuse or tax avoidance)

2. X has been engaged in one or more of the following:

   (a) Fraudulent evasion[2];
   (b) Conduct caught by the General Anti-Abuse Rule[3];
   (c) Conduct caught by the Halifax Abuse principle[4];
   (d) Entered into arrangements caught by a DOTAS or VADR scheme[5];
   (e) Conduct caught by a recognised 'anti-avoidance rule'[6] being a statutory provision which targets arrangements where either a main purpose, or an expected benefit, is to obtain a tax advantage or where the arrangement is not effected for commercial purposes. 'Targeted

[1] https://www.iasplus.com/en/standards/ifrs/ifrs10
[2] 'Fraudulent evasion' means any 'UK tax evasion offence' or 'UK tax evasion facilitation offence' as defined by section 52 of the Criminal Finances Act 2017 or a failure to prevent facilitation of tax evasion under section 45 of the same Act.
[3] "General Anti-Abuse Rule" means (a) the legislation in Part 5 of the Finance Act 2013; and (b) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions
[4] "Halifax Abuse Principle" means the principle explained in the CJEU Case C-255/02 Halifax and others
[5] A Disclosure of Tax Avoidance Scheme (DOTAS) or VAT Disclosure Regime (VADR) scheme caught by rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Section 19 and Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Section 19 and Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.
[6] The full definition of 'Anti-avoidance rule' can be found at Paragraph 25(1) of Schedule 18 to the Finance Act 2016 and Condition 2 (a) above shall be construed accordingly.

Anti-Avoidance Rules' (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;

(f) Entered into an avoidance scheme identified by HMRC's published Spotlights list[7];

(g) Engaged in conduct which falls under rules in other jurisdictions which are equivalent or similar to (a) to (f) above.

Condition three (Arrangements are admitted, or subject to litigation/prosecution or identified in a published list (Spotlights))

3. X's activity in *Condition 2* is, where applicable, subject to dispute and/or litigation as follows:

(a) In respect of 2(a), either X:

(i) Has accepted the terms of an offer made under a Contractual Disclosure Facility (CDF) pursuant to the Code of Practice 9 (COP9) procedure[8]; or,

(ii) Has been charged with an offence of fraudulent evasion.

(b) In respect of 2(b) to (e), once X has commenced the statutory appeal process by filing a Notice of Appeal and the appeal process is ongoing including where the appeal is stayed or listed behind a lead case (either formally or informally). NB: Judicial reviews are not part of the statutory appeal process and no supplier would be excluded merely because they are applying for judicial review of an HMRC or HMT decision relating to tax or national insurance.

(c) In respect of 2(b) to (e), during an HMRC enquiry, if it has been agreed between HMRC and X that there is a pause with the enquiry in order to await the outcome of related litigation.

(d) In respect of 2(f) this condition is satisfied without any further steps being taken.

(e) In respect of 2(g) the foreign equivalent to each of the corresponding steps set out above in 3(a) to (c).

For the avoidance of doubt, any reference in this Annex 1 to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time including any implementing or successor legislation.

[7] Targeted list of tax avoidance schemes that HMRC believes are being used to avoid paying tax due and which are listed on the Spotlight website: https://www.gov.uk/government/collections/tax-avoidance-schemes-currently-in-the-spotlight

[8] The Code of Practice 9 (COP9) is an investigation of fraud procedure, where X agrees to make a complete and accurate disclosure of all their deliberate and non-deliberate conduct that has led to irregularities in their tax affairs following which HMRC will not pursue a criminal investigation into the conduct disclosed.

HM Revenue & Customs

HMRC Tier 1 and 2 Model ICT Contract

Version 2.3 (November 2020)

SCHEDULE 2.1 | Services Description

Schedule 2.1 | BACKGROUND AND INTRODUCTION

1. INTRODUCTION

1.1. This Schedule sets out the following:

Part A: Description of Output Services

Part B: Description of Input Services

Part C: Description of Email & Mobile Messaging Services

Part D: Transition

DEFINITIONS

1.2. INTRODUCTION TO THE AUTHORITY

1.2.1. HMRC is the UK's tax, payments and customs authority, and it has a vital purpose: to collect the money that pays for the UK's public services and help families and individuals with targeted financial support.

We have five strategic objectives that guide everything we do:

(a) collect the right tax and pay out the right financial support;
(b) make it easy to get tax right and hard to bend or break the rules;
(c) maintain taxpayers' consent through fair treatment and protect society from harm;
(d) make HMRC a great place to work;
(e) support wider government economic aims through a resilient, agile tax administration system.

1.2.2. Communicating effectively through the right channels is at the heart of the service HMRC provides to its customers. The services being procured are therefore central to HMRC being modern and trusted. Meeting the service standards laid out is critical to the Department's relationship with the customer and the effective collection of tax and payment of benefits and must therefore always be the supplier's prime focus.

1.2.3. We are on a Transformational journey driven by a number of complimentary major programmes of work with whom the supplier will be expected to both interact and to provide expertise when it comes to communicating with customers. The supplier's ability to

bring innovation into the Customer Communication Services being procured will also be important in supporting our digital ambitions and driving efficiency.

1.2.4. We will be keen to exploit options to present the outputs we provide currently in paper format into alternative digital formats though the customers' digital accounts and through the HMRC App. We are keen to explore the options for increasing the accuracy of the positioning of scanned post into right post queues as well as increasing options of automation responses to incoming customer correspondence. We are also keen to unlock the wider benefits of emerging technologies such as RCS and AMB when constructing a truly seamless omnichannel customer experience. **REDACTED**.

1.2.5. The Authority is actively looking at:

(a) further utilising the Authority's current strategic document composition solution (**REDACTED**) for multi-channel customer communications to facilitate the paper to digital channel shift;

(b) improved management of undelivered SMS and email;

(c) improvements to the subscription service, such as resubscribe;

(d) management information data and admissible evidence;

(e) alternative messaging capabilities;

(f) proposed use of RCS and AMB (Apple Messaging for Business);

(g) two-way messaging/communications capabilities;

(h) **REDACTED**;

(i) interacting with customers based on their communication preferences;

(j) personalised communications.

1.3. CHANNEL STRATEGY

1.3.1. HMRC has been on a digital journey for many years. There are a range of factors that influence channel shift and HMRC will be looking for advice and support in increasing the pace of channel shift through this contract. **REDACTED**.

1.3.2. **REDACTED**

2. CROSSCUTTING REQUIREMENTS

2.1 The Supplier shall ensure that all processing, storage and transmission (in so far as the external endpoint of the Supplier solution) is based within the UK.

2.2 The Supplier shall ensure that all support personnel are located within the UK and hold the appropriate security vetting for the categories of data (e.g., PII, HCI, Secret and Top Secret) to which they may be exposed or have access (see Clause 14.1(b)(ii)).

2.3 The Supplier shall issue invoices to the Authority every month for each Service area in respect of the Run Service Charges and any other applicable charges. The number of invoices required will vary throughout the duration of the Contract and the Supplier shall adjust its invoicing practices accordingly. The Authority provides below an indication of an average month for each service area; however, this may change during Transition and over the course of the Contract:

(a) Output Services – fifteen (15) invoices per month;
(b) Email and Mobile Messaging – fifteen (15) invoices per month;
(c) Input Services – six (6) invoices per month.

2.4 **SUPPLIER KEY ROLES**

Service Management

2.4.1 Dedicated service management provision is required to facilitate business as usual activities, service performance and monitoring, general queries, incident management, technical support, change activities and regular service reviews, including performance reviews.

2.4.2 The Supplier shall provide a contact who will pro-actively liaise with the Authority and attend regular and ad-hoc checkpoint calls to keep the Authority informed of any issues with quality, processes and identify any risks to delivery, ensuring these are resolved promptly.

2.4.3 Attendance and participation at full end to end supply chain meetings (including mail service providers) is also required. These meetings are held quarterly, with an increase in frequency to monthly during peak periods and/or where required.

Account Manager

2.4.4 The account manager is to embody the relationship between the Supplier and the Authority by promoting a shared understanding of the Authority's aims, priorities, and deliverables across the organisation of the Supplier. The account manager is required to act as an escalation point for issues, promote, and champion continuous improvement and change. In addition, the account manager is required to monitor risk, and is responsible for the Supplier's

input to the Joint Business Plan, and the Supplier's Disaster Recovery and Business Continuity plans. The account manager is the strategic partner representing the Supplier. As such, the account manager must have experience of this role and be able to demonstrate where they have added value to a strategic partnership such as this, preferably with a government department or similar large-scale organisation.

2.5 DIGITAL ACCESSIBILITY

2.5.1 The Authority is required to ensure all digital services/products purchased from suppliers and/or operated by the Authority meet public sector accessibility regulations. The regulations state that the product or service being delivered through a web browser or mobile applications must be WCAG 2.1 AA compliant.

2.6 SECURITY REQUIREMENTS

2.6.1 Further details of the Authority's security requirements can be found within Appendices A-G of the Security Plan included within the Supplier's tender response. (Tenderers should note that this document can be found within the tender event) as well as within the links below here:

(a) *https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework;*

(b) *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf.*

2.6.2 Security clearance levels of personnel will be determined post Contract award.

2.6.3 Security clearance ("SC") is required for the Supplier's personnel where they, in their role, will have access to the Authority's systems and where they may have enhanced controls or ability to amend configuration within the systems.

2.6.4 Throughout the life of the Contract, the Authority reserves the right to conduct audit checks to make sure the Supplier's personnel are vetted at the stated security level required.

2.6.5 The Authority reserve the right to conduct security on-site reviews to ensure the Supplier's physical estate and processes meet the requirements detailed in this document. The Authority will provide advanced notice and agree a specific date with the Supplier before conducting a visit.

3. PART A: Description of Output Services

3.1. INTRODUCTION TO OUTPUT SERVICES

Service Overview

3.1.1 Transactional, Composition Required and Form Fulfilment are the three main types of print output required. These are comprised of the following and the Supplier shall accept:

(a) Transactional print (see Appendix 1 - Process Maps) (**REDACTED**):
  (i) print ready file; and/or;
  (ii) file containing the attributes (**REDACTED**).

(b) Composition required prints:
  (i) raw data file;
  (ii) file containing the attributes;
  (iii) artwork.

(c) Form Fulfilment:
  (i) print ready file;
  (ii) specific product;
  (iii) service catalogue requests;
  (iv) non-catalogue requests.

3.1.2 Quadient is currently the Authority's chosen strategic document composition tool for transactional and hybrid mail. The Authority will utilise this tool further during the lifetime of the Contract to bring more capability in-house and to centralise customer correspondence, allowing for increased channel shift opportunities. The Supplier shall support this journey and to work in collaboration with the Authority to innovate the Service and support a move towards full multi-channel communication.

3.1.3 It will be the Supplier's responsibility to prioritise workloads to ensure outputs are despatched on time and in accordance with SLAs. This includes where multiple jobs need to be produced in high volume in peak periods. **REDACTED**. The Authority will not pay for overtime costs incurred by the Supplier unless it has been pre-approved by the Authority. This is expected to only be in exceptional circumstances, for example when the Authority requires an urgent, high priority Bespoke mailing. In such instances, the Authority will

discuss with the Supplier the requirements and timescales and will endeavour to provide 48 hours' notice to allow the Supplier time to arrange the resource required.

3.2. **SERVICE REQUIREMENTS**

Collaboration

3.2.1. The Supplier shall work collaboratively with the Authority and the Authority's supply chain to enable an efficient end-to-end experience. This will include but is not limited to:

(a) IT provider(s), for example regarding exchange of print files and data;

(b) mail service suppliers, for example around consumables and ensuring smooth and timely despatches of outputs.

Transactional Print

3.2.2. There are three transactional print categories:

(a) **Category 1** – For outputs where it is critical that they land with the Authority's customers on a certain day and in certain volumes to support the Authority's Key Business Events;

(i) the Supplier shall make ready for collection and despatch specific outputs to the relevant postal provider(s) on specific dates and volumes;

(ii) the Authority will specify the products, dates and volumes of outputs per day to be despatched by the Supplier. The Authority will communicate this to the Supplier via use of 'despatch profiles' (**REDACTED**);

(iii) despatch profiles are signed off following the monthly Outputs Planning & Governance Board. The Supplier shall attend the Outputs Planning & Governance Board. It is expected the Supplier will advise if planned outputs are able to be produced. The Supplier is to highlight any issues that may prevent the Supplier from being able to produce and make ready for collection and despatch the planned outputs. The Supplier shall review progress against despatch profiles at least twice weekly in a joint meeting with the Authority;

(iv) upon receipt of the print ready files, where numbers vary significantly from forecasts, the Supplier must notify the Authority to agree a required/revised despatch so the Authority's contact centre forecasting can be effective;

(v) the Supplier shall be flexible if there is a need for the Authority to change the specified volumes and dates of despatch. Please refer to the Changes, cancellations, Pauses and Stops to Print Requirements section;

(vi) **REDACTED**.

(b) **Category 2** – *For outputs that are time critical;*

(i) outputs will be despatched within the performance indicators and in line with the Output Handling Instructions (**REDACTED**). Where numbers vary significantly from forecasts, the Supplier shall notify the Authority to agree a required/revised despatch so the Authority's contact centre forecasting can be effective;

(ii) **REDACTED**.

(c) **Category 3** – This will be the default category for all other outputs which do not meet the criteria of the Category 1 & 2 and the Supplier has the discretion to manage the print production and despatch of Category 3 outputs within the limits of the performance indicators;

(i) outputs will be despatched within the performance indicators and in line with the Output Handling Instructions (**REDACTED**).

(d) **Table A: REDACTED**.

REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**

REDACTED.

3.2.3 Inserts - The Supplier shall produce inserts (see Forms Fulfilment section) and include these with the applicable products as per the Output Handling Instructions.

3.2.4 **REDACTED**.

File Information

3.2.5 The following in relation to File information shall apply:

(a) some files sent by the Authority may have been merged to reduce the number of smaller files being sent to the Supplier;

(b) if the Supplier wishes to merge any files received, prior written agreement must be obtained from the Authority as there can be significant risks with the merging of files from the Supplier's perspective, particularly where file sources could be from different Heads of Duty systems ("HODs"). Requests to merge files may not be approved;

(c) all files will be sent to the Supplier via the Authority's approved inbound connectivity pathways including DES (Data Exchange Service), SDES (Secure Data Exchange Service) and IF (Integration Framework). Details can be provided upon request to assist the Suppliers' solution design.

3.3. HMRC CENTRAL PRINT SERVICE ("HCPS")

3.3.1 HCPS is a hybrid mail service which allows the Authority's advisors to create and send letters to customers using standard templates (see Appendix 1 - Process Maps);

(a) letters sent using HCPS are time critical. **REDACTED**. A consolidated file will be sent each day and the Supplier shall meet the SLAs for HCPS and print and despatch letters on the same day as file receipt;

(b) the Supplier shall provide an automated digital handshake to the Authority on each file received once processed and fulfilled;

(c) the Authority shall reconcile daily outputs with the Supplier, updating the status of the print item when feedback on each file is received from the Supplier;

(d) **Table B**: **REDACTED**.

REDACTED	**REDACTED**

REDACTED	**REDACTED**
REDACTED	**REDACTED**
REDACTED	**REDACTED**
REDACTED	**REDACTED**

3.4 COMPOSITION REQUIRED

3.4.1. The Supplier shall compose raw data (transferred by the Authority via the SDES) and artwork into a print ready state ready for production as per the attributes.

3.4.2. Print and package the outputs and make output ready for collection and despatch in line with the performance indicators.

3.4.3. There are 2 types of composition, Bespoke Mailings and Business as Usual Composition Products:

Bespoke Mailings

(a) Bespoke Mailings (see Appendix 1 - Process Maps) are a one-off output produced in bulk to a ringfenced customer group for a particular purpose outside of transactional print activities, **REDACTED**:

(i) **REDACTED**.

3.4.4 **REDACTED**.

3.4.5 The Supplier shall provide flexibility and good time management to ensure Bespoke Mailings are issued to agreed timescales in short notice (usually less than one (1) month) and quantities for specific despatch dates.

3.4.6 Volumes typically range from approximately fifty (50) thousand to one point four (1.4) million per mailing. However, this may on occasion need to be substantially more (for example, the entire taxpayer population of approximately sixty (60) million).

3.4.7 The Authority recognises there may be a need for the Supplier to procure resources in volume (such as paper) at short notice to meet requirements for Bespoke Mailings. Requirements and payment timescales will be discussed at the time of the request for any Bespoke Mailings of significant size (1m+).

3.4.8 ***Table C*** – **REDACTED**

REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED

Business as Usual Composition Products

3.4.9 These include NEP (New Employer Pack) letters and RTI (Real Time Information) mailings. **REDACTED**.

3.4.10 Historic volumes for Financial Year 21/22:

REDACTED

Payable Orders

3.4.11 The Supplier must (see Appendix 1 - Process Maps) **REDACTED**:

(a) be able to receive raw data from our Payable Orders (including payslip booklets) HODs;

(b) provide document composition development services to support the creation of output in the Authority's composition software print and package the outputs;

(c) make ready for collection and despatch in line with the performance indicators;

(d) produce all Payable Orders to conform to Pay.UK Standards such as the material; layout, print specifications and specialist inks;

(e) be accredited under the C&CCC (Cheque and Credit Clearing Company) Cheque Printer Accreditation Scheme (CPAS) and fully conversant with Cheque and Credit Clearing Company Standards.

3.4.12 The Authority envisages in the future to provide print ready files for Payable Orders in line with transactional print file formats.

3.4.13 **Table D**: **REDACTED**

REDACTED	**REDACTED**
REDACTED	**REDACTED**
REDACTED	**REDACTED**

3.5. **FORM FULFILMENT**

General requirements

3.5.1. The Supplier must:

(a) produce a number of different types and volumes of products required by the Authority which can include forms, inserts, notes, booklets, flyers and any form of printed stationery/ guidance/ business cards also miscellaneous items including printing and binding, labels, also bespoke/personalised items such as plaques, pens, banners etc;
(b) receive orders for such products;
(c) receive artwork and templates from the Authority and produce those products;
(d) process requests to change products;
(e) make output ready for collection and despatch orders in accordance with the requirements outlined in section 3.19 'Packaging and Despatch of the Output' and the performance indicators;
(f) use a print-on-demand approach as the default position and use intelligent stock control where applicable to ensure there are no shortages and/or unnecessary excess;
(g) fulfil cost-efficient processing of orders;
(h) provide clear and transparent stock management that covers the life of the form or product, from beginning to end;
(i) provide storage for stock.

Types of products and Volumes

3.5.2 The Authority requires the Supplier to:

a) produce a number of different types and volumes of products and there are approximately 563 products the Authority may require the Supplier to produce (see Appendix 1 – Process Maps);

b) **Table E**: *Historic approximate order lines received.*

REDACTED	**REDACTED**
REDACTED	**REDACTED**
REDACTED	**REDACTED**
REDACTED	**REDACTED**

3.6 SPECIFIC PRODUCTS

Business Cards

3.6.1 The Supplier must:

(a) produce business cards on a template provided by the Authority that can be personalised by using information provided by a user from the Authority;

(b) receive requests from the Authority's users via myBUY and allow documentation to be attached to the request if needed (as determined by the Authority);

(c) despatch using the Authority's preferred postal courier.

Giro Slips and Covers (V111)

3.6.2 The Supplier must:

(a) produce giro slips in accordance with the specification supplied by the Authority, to enable customers to make payments to the Authority;
(b) giro slips must have a magnetic strip;
(c) volumes are approximately one (1) thousand every six (6) months;

(d) specification:

(i) **REDACTED**

3.7 **ALCOHOL DUTY STAMPS LABELS**

3.7.1 The Supplier shall print alcohol duty stamp labels as detailed in: **REDACTED**.

3.7.2 The Supplier shall integrate the ordering process with the Authority's registration and certification processes for alcohol duty stamps.

3.7.3 The Supplier shall provide a means for the Authority's customers to order alcohol duty stamps (currently online ordering website).

3.8 **ORDERS**

3.8.1 **Service Catalogues – for orders required by users from the Authority**

(a) The Authority's users will request volume(s) of forms via MyBUY which will route through to the Supplier to be fulfilled;

(b) In order to allow the Authority to submit orders and for the Supplier to receive orders, the Supplier must provide the Authority with catalogues in full to support the provision of the Services and be able to comply with the Authority's MyBUY payment processing system with immediate effect. The Supplier shall provide and maintain the catalogues of products which must be in a user-friendly format. The catalogues will belong to the Authority;

(c) By the end of the transition period, the Supplier must provide the Authority with the catalogues for the full list of products (**REDACTED**). The catalogue shall include at least details of pricing, item product code (naming conventions for these products will be agreed with the Authority) and an image in jpeg format to assist the Authority's users in identifying each item. The Authority will provide the necessary artwork and details for each product to be included.

3.8.2 **Non-Catalogue Requests**

(a) The Authority's users must be able to request miscellaneous / bespoke items from the Supplier that are not available on the service catalogue. Miscellaneous items include printing and binding, labels, and bespoke/personalised items such as plaques, pens,

banners etc. The Supplier must be able to receive these as non-catalogue requests via MyBUY and fulfil these orders;

(b) Users from the Authority need to ensure they have obtained permission from the dedicated team within the Authority (the Mail Services Team at the time of signing this Contract) before submitting a non-catalogue request, and the Supplier shall ensure this approval has been obtained before proceeding to fulfil the non-catalogue request. The Supplier shall liaise directly with users from the Authority to agree requirements and specification of the non-catalogue request, including timescales and despatch method. The Supplier shall provide confirmation to the dedicated team within the and the user within the Authority who submitted the non-catalogue request, when the non-catalogue request has been fulfilled;

(c) Costs for non-catalogue requests must align to the contractual rates for all of the relevant component parts, including, but not limited to, the price for the appropriate paper and printing.

3.8.3 **Ordering process – for orders received from the Authority's customers via the Authority's contact centres and/or GOV.UK**

(a) The Authority has provision for its customers to order and receive printed copies of forms via its contact centres. The Supplier shall fulfil this provision;

(b) Orders for forms will be sent daily (**REDACTED**) to the Supplier via SDES;

(c) The Supplier must provide confirmation of receipt of the file(s) via SDES.

3.9 **ARTWORK AND PROOFING**

3.9.1 The Supplier shall accept print-ready PDF artwork from the Authority.

3.9.2 The Authority will supply new and updated versions of print-ready PDF artwork as and when these are required.

3.9.3 The Supplier shall provide a PDF proof of the test print back to the Authority usually within 48 hours for quality assurance.

3.9.4 Once artwork is agreed, the Supplier shall print and produce the artwork.

3.9.5 For new products the Authority will specify the volume of forms required to be printed for the first run.

3.10 CHANGES TO PRODUCTS

3.10.1 The Authority will aim to provide a minimum of three (3) months' notice as standard for when updates will become effective to documentation.

3.10.2 The Supplier shall provide flexibility and good time management to ensure urgent changes to forms are completed to agreed timescales at short notice (as little as three (3) or four (4) weeks) and ensure quantities required.

3.10.3 On critical occasions, notice may be limited to two to three (2-3) days, for example, changes to forms required following Budget announcements. The Supplier shall work with the Authority to expedite production of forms urgently as and when required.

3.10.4 When new stock is required due to new artwork:

(a) the Authority will send a 'copy stop' notice to the Supplier. Upon receipt, the Supplier shall immediately stop any further copies of previous versions from being printed;

(b) the Authority will instruct the Supplier on the print purchasing enquiry ("PPE") (**REDACTED**) if any existing stock is required to be either used to exhaustion or destroyed before the new stock is used;

(c) upon receipt of the PPE the Supplier shall provide a price to the Authority for the product based on the specification and in line with the contractual pricing within the agreed rate card;

(d) the Authority will review and approve/reject the completed PPE as appropriate and return to the Supplier. If the PPE is rejected, the Authority and the Supplier shall discuss the reasons for rejection and work together to resolve;

(e) upon receipt of the approved PPE, the Supplier shall process the request to produce the new form, and store any associated stock;

(f) the Authority will provide the Supplier with a 'deletion notice' and the Supplier shall delete old/previous versions of the form from the catalogue (unless there is a retention period required, as advised to the Supplier by the Authority).

3.11 INTELLIGENT STOCK CONTROL

3.11.1 The Supplier shall use intelligent stock control to ensure there are no shortages and/or unnecessary excess.

3.11.2 In the event of there being any unused excess where circumstances are within the Supplier's control the cost shall be borne by the Supplier.

3.11.3 The exception to the above is:

(a) where the Authority may bear the costs of wastage for obsolete/ redundant stock if the minimum notice period of three (3) months for changes to forms is not given. For example, if the typical requirement in three months is 10,000 units and the Authority gives the Supplier a three (3) months' notice, if the Supplier's stock holding is 150,000 units the Authority will not bear the wastage costs of the surplus 140,000 and the costs for destruction must be borne by the Supplier;

(b) for certain products, such as Self-Assessment notes and forms, the Authority requires the Supplier to retain a specified amount of stock and the Supplier shall do so, for each financial year, for current year plus 4 years. The amount of stock to be retained for each year will be any surplus stock printed for the particular financial year's print run. Past financial year's forms must be available to be requested by customers. At the beginning of the new financial year, stock dated current year minus four (4) years shall be detailed to the Authority and shall be destroyed in agreement with the Authority.

3.11.4 The Authority envisages further digitisation of forms in future and less requirement for forms to be printed. The Authority will work with the Supplier to supply intelligence as to future requirements for individual products which may change, to allow the Supplier to apply this intelligence to their processes, which the Supplier shall do, particularly where there is agreement between the Authority and the Supplier for forms to be pre-printed in advance.

3.12 **COST-EFFICIENT PROCESSING**

3.12.1 The Supplier shall fulfil all orders for forms in the most cost-efficient way for the Authority. This includes paper, packaging and preparation for despatch, including despatch method.

3.12.2 **Clear and transparent stock management** - The Supplier shall provide stock management that covers the life of the form or product, from beginning to end. For example, if 500 thousand booklets are printed for a particular requirement based on best estimated volumes, but only 450 thousand of those booklets are used, the Supplier shall clearly make visible to the Authority the remaining 50 thousand and the current position (i.e., retained as stock, to be destroyed, etc).

3.13 STOCK HOLDINGS AND STORAGE REQUIREMENTS

3.13.1 The Supplier shall accept current stock holdings from the incumbent supplier (if applicable), and store these until such time as despatch is required. The Supplier must be able to despatch this stock in line with agreed processes, and shall do so, without charging the Authority for the production of this stock, as the stock will already have been paid for by the Authority. The Supplier must work with the incumbent supplier to arrange secure transit of the current stock holdings on times and dates to be agreed as part of the Transition Plan. Where there is existing stock of forms fulfilment items, once the existing handed over stock has been exhausted, the Supplier shall apply the pricing agreed with the Authority (whether as part of contract award or during transition) for each of the items required.

3.13.2 Current storage requirements for all forms are approximately 89 pallets and 553 bins worth of stock, equating to approximately 4,200 square feet.

3.13.3 Storage requirements for all other stock including inserts and envelopes equates to 733 pallets and an approximate area of 7,432.62 square feet.

3.13.4 The Supplier must ensure that all stock is stored in a suitable and secure environment, where it cannot be damaged or deteriorated. The storage area must meet the requirements of the national Health and Safety at Work Legislation. The environment must be regularly monitored and assessed to ensure that standards are maintained.

OTHER AD HOC SERVICES

3.13.5 **Child Benefit material distribution**: The Supplier shall arrange targeted distribution of materials (produced by the Supplier under the form fulfilment requirement in this schedule), relating to Child Benefit, with the aim of ensuring optimal number of parents of new-born children receive material from the Authority making them aware of their entitlement to claim.

3.13.6 **Legal proceedings printing and bundling:** The Authority's 'Solicitor's Office & Legal Services', may require the Supplier to provide document printing and bundling, typically at very short notice (as little as 12 hours turnaround time). Used for legal proceedings, these bundles can comprise thousands of pages, with numerous copies required. The Supplier must be positioned to and shall handle last-minute requests. The method of data transfer will be determined at the time of the request. Where documents are held digitally, the Authority will transfer the files to the Supplier via SDES.

3.13.7 **Supreme Court cases printing and bundling:** On occasion, the Authority may require the Supplier to provide document printing and bundling, as outlined above, for (less frequent) Supreme Court cases. In doing so, the Supplier must follow the relevant Supreme Court practice directions and electronic bundle guidance.

3.13.8 In both instances, the content will be provided by the Authority and the Supplier shall produce the bundles to specific requirements (set out by the Authority), and then shall either return the bundles to the Authority, and/or deliver them to a specified location within a specified timeframe.

3.13.9 **Bespoke Welsh language products:** The Supplier shall provide a provision for Welsh language products to be produced, such as booklets, banners and PDF documents, where familiarity with the nuances of the Welsh language is required. For instance, how special characters and words with a greater number of characters than English can affect the formatting and layout of the output. For all outputs, where required, the Supplier shall print in Welsh, including two characters specific to the Welsh language, circumflex 'ŵ' and circumflex 'ŷ'.

3.13.10 The Supplier shall support requests and produce such outputs at short notice, often as little as 24 or 48 hours for production at no extra cost.

3.14 CHANGES, CANCELLATIONS, PAUSES AND STOPS TO PRINT REQUIREMENTS

3.14.1 A request to change/cancel print/ pause production/ stop print may apply to any type of print as listed in this specification document.

3.14.2 The Supplier shall act with urgency to implement any requests from the Authority to change/cancel print/pause production/stop print. This is due to potential consequences that may be incurred by outputs being received by customers that should not have been despatched, including reputational damage and legal implications (for example if the outputs concerned are legal documents being sent to customers).

3.14.3 The Authority recognises the impacts to the Supplier of such a request, on resource, production materials and planning, and will endeavour to keep such requests to a minimum and only where necessary.

3.14.4 In the event of such a request, the Authority will keep in close communication with the Supplier and advise of actions the Supplier is required to take. The Supplier must act on written instructions from the Authority and not act outside of any instruction from the Authority. For example, if the Authority requests for any or all production to be stopped, the Supplier must not destroy any output until it has had a specific instruction in writing from the Authority to do so. The Authority is aware of the challenges that such requests can

cause for the Supplier and will endeavour to advise the Supplier urgently of the actions they are required to take.

3.14.5 *Changes to print requirements* – The Supplier shall accommodate multiple requests for changes from the Authority either to print product content and/or how and when they are despatched whilst products are in development. There may be occasions when the Supplier is required to accept changes to print products after the Authority has provided confirmation of the requirement or even during production. These include (but are not restricted to):

(a) Category 1 outputs, where a despatch profile has already been submitted to the Supplier. Notice may be several weeks in advance or at short notice (24 hours). Changes to despatch profiles may be (but not always) as a result of incident management actions (see section 3.29) which the Supplier may be required to support. The majority of despatch profiles are unlikely to change;

(b) Bespoke Mailings - volumes, number of product types and frequency of despatch may all change even after confirmation of the requirement has been provided to the Supplier. This is usually due to data refinements that more accurately identify the number of customers affected who require an output. **REDACTED**.

3.14.6 *Cancel print* – Requests to cancel print may be required and print shall be cancelled by the Supplier when the output is pre-production and the print files have been received by the Supplier but post confirmation to the Supplier of the details of the mailing. Examples of where the Authority may request to cancel print could include:

(a) Bespoke Mailings where the order has been confirmed;

(b) Category 1 outputs where a despatch profile has already been submitted to the Supplier and where a decision has been made that the Authority should not send the output – this is expected to be rare.

3.14.7 *Pause production* – Where it is recognised by the Authority that print files are being processed and are at various stages of production, including printing stage or enveloping stage, and the Authority requires the Supplier to pause production for a temporary period, the Supplier shall pause print. The intention of asking the Supplier to pause print is where it is likely that the Authority will later advise the Supplier for production to continue, but a pause is required to allow time for the Authority to investigate any issues that have occurred in the Authority's processes. To ensure continuity of production, the Authority and the Supplier may come to an agreement in any such event that outputs mid-cycle may continue to be processed and finalised to the end of the particular stage they were at when the request was made. For

example, if 20 thousand out of 40 thousand outputs had been enveloped, the Authority is likely to agree for the remaining 20 thousand to be enveloped, so as to free up the enveloping machine for the Supplier and prevent running the whole file through the printing and enveloping process again as and when production resumes.

3.14.8 *Stop print* – Where it is recognised by the Authority that the outputs are incorrect, and production needs to stop immediately, regardless of at what point in the production cycle the outputs are, the Supplier shall stop print. It is unlikely that the outputs will need to be restarted, and for any outputs already produced it is likely that the Authority will require them to be destroyed by the Supplier.

3.14.9 Where the request is to stop individual outputs, the Authority recognises the challenges such a request can pose and the Supplier shall work with the Authority to implement a suitable solution should the need arise.

3.14.10 The Supplier shall identify, extract and destroy specific outputs at the request of the Authority, when required. It is expected that these requests will be rare.

3.14.11 Where the request is made by the Authority to:

(a) make changes to print requirements – no charges shall be incurred by the Authority;

(b) cancel print, i.e., to destroy print files have not yet been processed – no charges shall be incurred by the Authority. If paper and envelopes have already been purchased by the Supplier, these resources shall be used for other outputs required by the Authority;

(c) pause production and stop print - the Authority will pay for costs incurred as per the cost model for any product printed/enveloped, but not for product not yet printed/enveloped.

3.14.12 Further, if there is a need to quarantine the output for a period of time, for example, to allow the Authority to undertake investigation which may result in the output being despatched, depending on the volume of the printed output, the Authority may pay storage costs where these costs are incurred.

3.15 PAPER AND ENVELOPE SPECIFICATION - OUTPUT SERVICES

3.15.1 The paper and envelope products supplied under this Contract shall meet the mandatory minimum standards set out in the Government Buying Standards in the following link and the Supplier shall provide proposals on their most sustainable offering:

http://www.gov.uk/government/publications/sustainable-procurement-the-gbs-for-paper-and-paper-products.

3.15.2 The Supplier shall ensure that all paper and all paper products must comply with the Timber Procurement Policy published by the Department for Environment, Food & Rural Affairs: https://www.gov.uk/guidance/timber-procurement-policy-tpp-prove-legality-and-sustainablity.

It is essential that the specifications below are met for security reasons, and Supplier shall meet them.

3.16 **PAPER – OUTPUT SERVICES**

3.16.1 The Supplier shall provide paper to the Authority's minimum standard for paper, which is 80gsm. However, there are exceptions as follows, and the Supplier shall comply with these:

(a) payable orders: to comply with Cheque and Credit Clearing Company Limited (C&CCC) banking standards the Authority's Payable Orders must be printed on 95gsm CBS1 quality paper;

(b) payslips: to comply with C&CCC banking standards the Authority's payslips must be printed on a minimum weight of 85gsm CBS2 quality paper.

3.17 **ENVELOPES**

3.17.1 The Authority is open to working with the Supplier to explore alternatives to enveloping, if there are benefits to adopting alternative methods. Until any such exploration is undertaken, the Supplier shall ensure envelopes are as follows and shall use envelopes which meet these criteria:

3.17.2 The Authority's standard default envelope is XDL (previously C5). The majority of products are sent in an XDL envelope, and it is expected that further products will have transitioned from being sent in a C5 envelope to be sent in an XDL envelope by the time of contract award.

3.17.3 Envelopes must be buff manilla and comply to the following:

REDACTED

3.17.4 On an exceptions basis the Suppliers may be required to use other envelopes (e.g., DL, C4) in line with the Output Handling Instructions. **REDACTED**.

3.17.5 The Supplier shall only use envelopes which are of a sufficient quality to ensure they remain intact during transit.

3.17.6 The Supplier shall ensure that for security reasons letter content will not be visible through envelope windows.

3.17.7 There are minimal outputs that require co-enveloping (as per the Output Handling instructions) but where outputs are co-enveloped the Supplier shall ensure outputs included in the envelope belong to the same customer and no cross-contamination with other customer outputs occurs.

3.18 SPOILS

3.18.1 The Supplier shall not charge the Authority for the production of spoils, nor the mailing of product not sent. The exception to this is where outputs already printed and/or enveloped but not yet despatched are not sent at the specific request of the Authority as outlined in the 'Changes, Cancellations, Pauses and Stops to Print Requirements' section.

3.19 PACKAGING AND DESPATCH OF THE OUTPUT

3.19.1 **General requirements**

(a) for all outputs, the Supplier shall use the most appropriate and cost-effective means of packaging and despatch using the appropriate mail service provider of the Authority. The Supplier shall be familiar with the postal market and shall continually review the most value for money method for the despatch of outputs;

(b) where the Supplier identifies that the most appropriate and cost-effective means of packaging and despatch is not currently being used, and to do so would enable savings for the Authority, the Supplier shall recommend to and work with the Authority to implement any necessary changes;

(c) the Authority is open to innovation in this area and exploring different types of packaging for outputs;

(d) requirements for the Supplier at the time of signing are:

(i) for transactional print and Payable Orders, the Supplier shall despatch outputs in accordance with the details held in the Output Handling Instructions;

(ii) the Outputs Handling Instructions detail that the Supplier shall envelope the majority of outputs, but there are a smaller number of outputs where the Supplier shall use alternative forms of packaging, including, padded envelopes, (lockable) crates and cardboard boxes sealed with secure seals as specified by the Authority;

(iii) the Supplier shall create Batch headers for printed output as per the Output Handling instructions;

(iv) the Supplier may be required to despatch outputs to addresses for other bodies, such as Chambers of Commerce or other government departments, and shall comply with any requests to do so;

(v) for Bespoke Mailings and products listed at 3.4.9 (Business as Usual Composition Products), the Authority will agree packaging and despatch requirements with the Supplier during the planning stages. Bespoke Mailings will typically be sent in a standard XDL envelope, but postal requirements may change depending on the urgency of the mailing. **REDACTED**

e) for forms fulfilment, the Supplier shall despatch the output into the appropriate mail services in agreement with the Authority. As a guide, these are:

(i) down Stream Access as the default service to despatch orders received and a Down Stream Access C4 envelope used;

(ii) the Supplier shall despatch orders being delivered to an office of the Authority, or international mail via the Authority's chosen mail service provider which provides delivery of mail between offices of the Authority (**REDACTED**);

(iii) if the order is not to be sent to an office of the Authority, and/or it cannot be sent in a C4 outer envelope, the Supplier shall despatch these as a parcel via the Authority's chosen mail service provider for parcels (**REDACTED**).

3.20 **SORTATION**

Software mailsort

3.20.1 The Supplier shall apply software mailsort for volumes of outputs wherever possible. The Supplier shall add a Mailmark barcode to the letter so that the barcode is visible in the window of the envelope. This allows Royal Mail to do an automated sort thus enabling the Authority to be eligible for Mailmark rates. See weblink below for specifications: https://www.royalmailwholesale.com/royal-mail-mailmark.

Hardware mailsort

3.20.2 The Supplier shall hardware mailsort outputs wherever possible where the Supplier is not able to software mailsort. This is usually where outputs are for customers who may live in remote areas or where there is poor address quality in the file. The Supplier shall apply a Mailmark barcode onto the envelope where possible.

Unsorted mail

3.20.3 Unsorted mail shall be managed in the following way:

(a) The Supplier shall process and send mail as unsorted that cannot be pre-sorted. This is usually due to poor address quality, including rejects from the sortation process;

(b) The Authority is keen to maximise the amount of mail that is software mailsorted and to work with the Supplier to achieve this where possible. It must be understood that the Supplier must not work in isolation to achieve this but must work with and obtain approval from the Authority regarding any proposed changes and improvements before implementation.

3.21 DATA VALIDATION

3.21.1 The Supplier shall provide data validation services to support with the Authority's ambition to reduce print volumes and decrease undelivered mail, for example, run raw data and print ready files against industry suppression lists such as Goneaways and deceased and improve address quality using the Royal Mails Postcode Address File.

3.22 MAIL SERVICE PROVIDERS – COLLABORATION AND INTERACTION

3.22.1 The Supplier shall collaborate with the Authority's mail service providers. Currently these are:

(a) **REDACTED**

for the avoidance of doubt, the Downstream Access license does not form part of this Contract:

(i) **REDACTED**

3.22.2 These are the providers at the time of Contract signing, however this may be subject to change throughout the lifetime of the Contract. The Authority will notify the Supplier of any changes if/when applicable and both parties shall work together to facilitate the change.

3.22.3 The Supplier shall ensure that any of their systems or processes critical to the injection of mail into Royal Mail's delivery stream are integrated with those of the Authority's Downstream Access provider or other mail providers for example, to upload manifests, volumes to be collected.

3.22.4 The Supplier shall pro-actively manage the relationship with the Authority's chosen mail service providers to submit accurate daily manifests to said mail service providers.

3.22.5 The Supplier shall undertake due diligence prior to bidding with the Authority's chosen mail service providers to identify to the Authority any technical or cost dependencies which may impact the ability of the Supplier to achieve integration. These costs must be included as part of bidding costs.

3.22.6 The Supplier shall work with the Authority's Downstream Access provider and other mail service providers to:

(a) ensure all the Authority's output goes out in line with the agreed Despatch Profiles and/or SLAs;

(b) ensure pallets are segregated into the Authority's Downstream Access provider's requirements and packaged suitably for despatch;

(c) **REDACTED**

(i) **REDACTED**

(d) accurately and timely forecast planned volumes for despatch including providing a rolling seven (7) day forecast and a 24-hour forecast once a day within agreed timescales and sending any necessary files to the Down Stream Access provider to enable this;

(e) accurately and timely submit manifests and emanifests with the relevant detail to the relevant mail service providers as required;

(f) support ordering of consumables such as trays, as required and in the volumes required;

(g) ensure the correct SCIDs allocated to the Authority are used (**REDACTED**);

(h) support with any changes that may need to be made to SCIDs.

3.22.7 The Supplier shall work with the Authority's chosen Down Stream Access provider to accommodate the Authority's larger mailings that need to be sent over a longer period (five (5) days+) so that the Authority do not incur charges from Royal Mail for issues around manifests being incorrect. Any solution to facilitate this must not be at any additional cost to the Authority.

3.22.8 The Supplier shall ensure the accuracy of the Down Stream Access manifest including the reconciliation of any entries relating to spoils to ensure postal charges are not incurred for any materials that are removed from the planned despatch and will be re-printed and despatched under separate production. The Supplier shall not charge the Authority for the production of spoils, nor the mailing of product not sent. Should the Authority incur additional postal charges due to errors within the manifest the Supplier shall refund these costs.

3.22.9 The Supplier shall ensure the accuracy of the Down Stream Access manifest to ensure the Authority's mail is not subjected to mail holds by Royal Mail, as a result of inaccurate or poor forecasting.

3.22.10 Where Royal Mail apply adjustment charges to the Authority for Unmanifested/Manifested Underpaid items, the Supplier shall work with the Authority's Downstream Access provider to identify failures in manifest uploads.

3.22.11 The Supplier must ensure that there is no loss or error in the handling of mail between the Supplier and the mail service provider(s). The Supplier must notify the Authority of any discrepancy and must be treated as a Breach of Security. In any such instances a full investigation and incident report must be supplied to the Authority.

3.22.12 The Supplier shall display agility in amending forecasts, reacting to print production changes and other external factors as necessary.

3.22.13 The Supplier may be required to input information to an online portal for the Authority's current International Mail provider (provider may be subject to change) and shall comply when requested to do so. Information could be as follows:

(a) customer reference – to be agreed;

(b) destination - Countries in the EU;

(c) weight break – select from a drop-down menu;

(d) number of items;

(e) total weight.

3.23 **COLLECTION TIMES**

3.23.1 The exact times of collection, including earliest and latest collection times, will have been confirmed between the Supplier and the Authority's mail service providers at the time of Contract commencement. Detailed conversations around any necessary changes shall occur during the Transition period.

3.23.2 The Supplier shall produce mail so it can be collected at multiple collection times throughout the day. Collection times agreed must ensure optimal despatch of outputs. The Authority recognises that location of the Supplier and distance of the Supplier from the Authority's chosen mail service provider chosen locations will be a consideration for the Supplier when agreeing collection times and arranging production to facilitate optimal collection.

3.23.3 The Supplier shall have outputs ready for collection and collections must be able to be made Monday to Saturday.

3.23.4 Collection times are expected to be as follows:

(a) earliest collection time is 07:00;

(b) last collection time to be no later than between 16:00 and 18:45.

3.23.5 The Supplier must have clearly highlighted any variance from the expected earliest and latest collection times as part of its bid response and have had that accepted by the Authority for any variances to these times to apply.

3.23.6 Once agreed, collection times can be changed only with prior approval of the Authority. The Authority is willing to consider building in some limited flexibility around collection times by allowing some minor variances that provide service improvements, efficiencies, or cost savings. This must also be clearly highlighted, explained, and evidenced to the Authority at the time of any such changes being submitted for agreement between the Authority and its

chosen mail service providers. For the avoidance of doubt, minor variances shall be plus or minus 30 minutes.

3.24 **MAILING PROPERTY & CONSUMABLES**

3.24.1 The Authority's mail service providers will be responsible for providing the Supplier, at the Supplier's agreed sites, with the use of the property and material required to undertake the Service obligations in the most efficient and cost-effective manner. Such property includes but is not limited to:

(a) mailing trays;
(b) label Printers (including PC(s), associated cables and internet connection where required, power supply unit, installation including connectivity and decommissioning);
(c) printer consumables;
(d) labels;
(e) postal manifest/docket books;
(f) tubs;
(g) bag ties;
(h) york containers, crates, racks/mail cages;
(i) elastic Bands.

3.24.2 The Supplier shall keep these items separate from other items to avoid them being inadvertently confused with other items not provided by the Authority's mail service providers. The Supplier shall order consumables for the required volumes to despatch the Authority's outputs as and when required.

3.24.3 The Authority experiences peaks and troughs of production throughout the year. To ensure that customers do not experience undue delays in receiving their mail, the Supplier shall work with the Authority's mail service providers to ensure that sufficient property and consumables are delivered, especially into any designated business critical sites of the Supplier. For example, there is a current requirement of 10,000 trays on site per day minimum. The Supplier shall work with the Authority's mail service providers to agree individual suitable provisions.

3.24.4 At the time of procurement, there is a requirement for the Supplier to shrink wrap pallets, however it is expected that in future this will no longer be a requirement as and when the Authority's chosen Down Stream Access provider moves to use of secure pallet lids with secure ties. The Supplier shall accommodate any changes to packaging of pallets as specified by the Authority's Down Stream Access mail provider and work with the Down Stream Access provider to implement as necessary.

3.25 SEEDING

3.25.1 The Authority uses Royal Mail's chosen provider for Seeding. **REDACTED**. The Authority will notify the Supplier of any changes if /when applicable and both parties shall work together to facilitate the change. The Supplier shall work with Royal Mail's chosen Seeding provider to facilitate the placing of identifiers within mail/outputs being despatched on a monthly basis and ad-hoc when required, so as to ensure Royal Mail quality of service for the Authority's mail can be measured across all mail sent via Mailmark products.

3.26 GENERAL REQUIREMENTS

3.26.1 Evidence of Output and Audit

(a) The Supplier shall provide full end-to-end traceability of all items, from receipt to despatch, providing a complete audit trail of all output, and robust enough to stand up in court;

(b) As a minimum, for individual outputs for individual customers to individual customer addresses, the Authority must be able to audit:

(i) data contained within the output sent to the Supplier by the Authority, such as name, address, postcode, National Insurance number, Unique Taxpayer Reference, etc;
(ii) when the file within which the output was contained was printed;
(iii) when the output was enveloped;
(iv) when the output was moved to the loading bay ready for despatch;
(v) when the output was despatched.

It is expected this information will be in the output metadata generated and held by the Supplier.

(c) The Authority is currently defining a strategic storage and retrieval solution to give the Authority greater access and visibility to the output metadata. The Supplier shall ensure they work with the Authority and support the migration of data if and when it intends to move forward with the solution. Any or all metadata held must be transferrable to the Authority at any point, in a format agreed with the Authority and the Supplier shall transfer such metadata when requested by the Authority. This may include requests for data for individual outputs despatched to individual customers and/or individual addresses;

(d) Until the new solution is in place, the Supplier must provide a service to retain Evidence of Outputs for a minimum of 7 years' worth of data (current year minus 6 years) using the most cost-effective solution possible. The Supplier must be able to auto-delete the information as specified by the Authority, e.g., on a rolling basis so as to retain only 7 years' worth of data. Moreover, this Service must be configurable to match specific business areas or needs e.g., Statutory Notices only (a specific list of products as specified by the Authority), certain outputs that require a 2-year retention period (as required by VOA for its Evidence of Outputs). If/when the new solution is in place, the retention of Evidence of Outputs by the Supplier will no longer be required.

3.27 **QUALITY CONTROLS**

3.27.1 The Supplier shall use best practice print methods to ensure quality and integrity of all output. This includes, but is not limited to, ensuring:

(a) outputs are printed accurately. For example, side A of the printed output must be for the same customer as side B (if side A does not match side B this would constitute a breach of security);

(b) customers receive the output intended for them (to not receive the correct output, or to receive incorrect output, would constitute a breach of security);

(c) print is clear and legible, free from smudging or unwanted marks;

(d) correct paper and ink specification is adhered to at all times;

(e) specialist outputs, such as Payable Orders, are printed to specification;

(f) envelopes are gummed and sealed correctly;

(g) whole address and barcodes are visible in the envelope window, and conversely no letter content is visible through the envelope window (thus constituting a breach of security);

(h) outputs are despatched in accordance with the Output Handling Instructions and to SLA.

3.27.2 The Supplier must ensure sample checking of a range of outputs is independently conducted on a quarterly basis, and outcomes sent to the Authority. The Authority will work with the Supplier to agree and implement suitable quality measures within three (3) months of contract award.

3.28 **SERVICE SUPPORT**

3.28.1 The Supplier must provide UK-based support. A dedicated helpdesk (telephone) and specific contact points (email)/escalation routes are required to resolve customer issues during the hours of Monday – Friday 07:00 – 20:00 and 07:00 – 16:00 on Saturday as a minimum. Please refer to incident management requirements.

3.29 **INCIDENT MANAGEMENT**

3.29.1 The Supplier's incident management procedures must meet and align with the priority levels outlined in Table F as a minimum. In this instance:

(a) the Supplier must report any incident when it is identified;

(b) the response time is the target time from the time an incident report is identified to the time an initial response is sent back to the Authority;

(c) the resolution time is the time that the Supplier commits to restore the service to a level acceptable to the Authority. The resolution time is calculated by a "stop the clock" approach whereby the clock is only paused or suspended when a query or question is directed to the Authority. The Authority reserves the right to work with the Supplier flexibly to adjust the resolution time dependant on the nature of the incident.

3.29.2 The Supplier shall provide support for issue resolution, regardless of whether the root cause lays with the Supplier, Authority, or both.

3.29.3 In instances where a P1 or P2 incident has been raised with the Supplier, the Authority requires investigation and resolution to continue outside of the above specified working hours, on a 24-hour basis, 7 days a week, 365 days per year and the Supplier shall provide this.

3.29.4 Incident management should cover anything which causes an interruption or a reduction in the quality of the service included but is not limited to security, IT and operational incidents.

3.29.5 The Authority will inform the Supplier immediately of any suspected Fraudulent Activity Incidents. Such incidents should be classed as Level P1, and the Supplier shall respond within the appropriate incident management priority level timescales.

Table F: *Incident Management priority levels*

Priority Level	Business Impact Summary	Response time	Resolution Time

Critical – P1	A complete outage where the Service cannot be accessed, affecting more than 75% of service or an incident that has a serious or reputational impact to the Authority	15 Minutes	4 Service hours
Major – P2	Service affecting or partial outage, including intermittent failures, affecting more than 50% of service or an incident that has a significant impact to the Authority	1 Hour	8 Service Hours
Minor – P3	Minor Service impact on system functions or affecting only single users. No direct impact on full service availability, or an incident that has minor impact to the Authority	6 Hours	2 Service Days
Low – P4	Low impact on the Service or system functions.	1 Business Day	3 Service Days
Low – P5	Low impact issue with single user or output.	1 Business Day	5 Service Days

3.30 **SUPPORT FOR COLLEAGUES WITHIN THE AUTHORITY**

3.30.1 From time to time the Authority will require the Supplier to support colleagues within the Authority. For example, this could be to help colleagues understand how the print operations work, or to enable a printed product to be quality checked.

3.30.2 The Supplier shall provide support including (but not limited to):

(a) hosting on site visits and tours of the print environment;

(b) information packs about the print environment, including size and scale, equipment used, facilities etc;

(c) virtual site tour.

3.31 **UPDATES AND UPGRADES**

3.31.1 The Supplier shall arrange any routine maintenance necessary so that it does not interfere with the achievement of getting the outputs despatched in line with the SLA.

3.31.2 The Supplier shall plan any software updates in advance, and release cadence shall be provided minimum six (6) months in advance. All planned maintenance must adhere to the Authority's change management policies ("CAB approval") and be submitted with appropriate forward notice period dependent upon the impact of any service outages along with details of an actionable regression plan.

3.31.3 In the event of an unsuccessful update, the Supplier agrees that consultation shall be within one (1) hour and the Parties shall agree remediation activities to restore service.

3.32 **CHANGE REQUESTS**

3.32.1 All Change Requests should be managed in line with the procedures set out in Schedule 8.3 (Change Control).

3.32.2 There are 4 types of change requests that may occur:

(a) contract change requests (see Schedule 8.3: Change Control Procedure);

(b) operational change requests, for example, a change to postal method;

(c) IT change requests, for example, producing a new Bespoke Mailing (**REDACTED**); and

(d) statement of work will be used on projects that do not sit under the 1, 2 or 3 (**REDACTED**).

3.33 **TESTING AND CONTROL GO LIVE PROCESS**

3.33.1 The Supplier must support, on requests throughout the life of the Contract, the Authority's testing requirements of existing or new printed outputs. The Authority will work with the Supplier to determine testing timeframes. The Supplier shall be flexible to support testing activities in condensed timeframes.

3.33.2 Testing can include:

(a) integration or network changes made by the Authority to ensure continuation of service;

(b) PDF sample proofs;

(c) print;

(d) print and fulfilment of prepared test files containing test data. In most cases the Authority will require the Supplier to scan and send digital copies of printed and enclosed test outputs but there may be instances where the Authority requires physical test outputs securely couriered to the Authority; and

(e) live production testing using live customer data where the Authority requires the Supplier to hold production until the Authority has signed off the first printed documents. In most instances this will be handled digitally by the Authority but there may be instances where the Authority will need to sign off the physical prints at a print site in person.

3.33.3 The Supplier must provide a pre-production environment to receive test print files from the Authority to remove risk of mixing live and test data. Print files supplied to the pre-production environments will contain a watermark.

3.34 MANAGEMENT INFORMATION (MI) AND REPORTING

3.34.1 The Supplier must provide accurate, complete MI with traceability to the Authority for all services and products, including those provided by Sub-contractors. It is the responsibility of the Supplier to provide the same level of MI from the Sub-contractors.

3.34.2 The Supplier shall provide data to the Authority as close to real-time as possible and in the format specified by the Authority. The content of the data provided shall be agreed upon by both parties.

3.34.3 The data required will consist of but is not limited to:

(a) date, time, volumes, name of products and HoDs to be provided for the following stages of the process:
  (i) file logging;
  (ii) production site(s), if applicable;
  (iii) despatch;
  (This information is required daily as a minimum)

(b) traceability of E2E customer journeys and supporting MI for evidence of outputs purposes (this information is required on request from the Authority and must be available within 48 hours maximum);

(c) updates to MI in the event of any changes, e.g., in the event of a request from the Authority to destroy files and not print, any data relating to items not printed must be reflected in the MI;

(d) performance measure reporting for all products (monthly as a minimum and to meet timescales specified by the Authority);

(e) stock volumes dashboard (information required is for volumes on hand per day, but is required weekly as a minimum);

(f) stock orders (this information required is for volumes of orders received per day, but is required weekly as a minimum);

(g) top 20 products for both transactional print and form fulfilment, including volumes, spend (this information is required monthly as a minimum).

3.35 **INVOICING**

3.35.1 The Supplier must invoice the Authority on a monthly basis via the myBUY system and provide consolidated invoices, where applicable, that detail the spend for each element of the services provided.

3.35.2 The Supplier shall not charge the Authority for images and/or pages that are blank.

3.35.3 The Supplier must produce a monthly audit that supports and accompanies the invoice(s).

3.35.4 The Supplier shall provide the Authority with signed proof of delivery notes detailing quantities received and printed product call offs.

3.36 **SECURITY**

3.36.1 **Physical security**

(a) the Supplier shall be accredited to ISO27001 for physical security standards (or working towards completing accreditation by contract award);

(b) the Supplier shall control access to secure areas within its premises where Authority data is stored and accessed and only persons with the designated roles and required security clearance levels must have access;

(c) where there are windows present in secure areas and such windows can be used to view inside the area, the Supplier must have obscuration film or blinds. The blinds must be maintained in good working conditions at all times;

(d) where there are windows present, the Supplier shall ensure that all windows have internal shutters that lock;

(e) the Supplier shall ensure that CCTV covers all areas where there are documents, and there must be no blind spots;

(f) the Supplier shall ensure that CCTV images captured in the premise are not obstructed or compromised in any way, including but not limited to being obscured by sunlight;

(g) the Supplier shall ensure that the boundaries of the site are clearly defined and marked. The Supplier shall ensure that the installation of CCTV cameras outside the premise are not obstructed or hindered by fencing or other obstructions. The Supplier shall ensure that adequate lighting is provided to ensure proper functioning of the CCTV cameras at all times. The Supplier shall ensure that the perimeter fencing is maintained in good condition to secure the premise;

(h) the Supplier shall ensure that the premises are equipped with an active fire suppressant system in accordance with all relevant fire safety regulations;

(i) the Authority reserve the right to conduct security on-site reviews to ensure the Supplier's physical estate and processes meet the requirements.

3.37 **DISASTER RECOVERY**

3.37.1 The Authority requires a minimum of dual site processing, and the Supplier shall provide this.

3.37.2 The Supplier shall have inter-site operability, with active flex and disaster recovery.

3.37.3 The Supplier should have reliable and robust disaster recovery capabilities to ensure no interruption to service. This should include the use of multiple geographically resilient datacentres and/or high availability patterns where cloud infrastructure is used.

3.37.4 In a Disaster Recovery situation, the Supplier must be able to stand up all services by the next Working Day.

APPENDIX 1: PROCESS MAPS - Output Services

Please note the below high-level process maps for illustration purpose only. Differences in process may occur on a product-by-product basis.

A) Transactional Print

REDACTED

B) HCPS - Output Services

REDACTED

C) Bespoke Mailing - Output Services

REDACTED

D) Payable Orders- Output Services

REDACTED

E) Forms Fulfilment - Output Services

REDACTED

APPENDIX 2 – PRODUCTION LEVEL ATTRIBUTES LIST- Output services

REDACTED

Appendix 3 – Example of IT Change Request-Output services

REDACTED

4. PART B: Description of Input Services

4.1. INTRODUCTION TO INPUT SERVICES

4.1.1. The Authority's drive is to increase efficiency, visibility, and flexibility to manage customer contact. To support this, the Authority is optimising digitalisation of mail, significantly reducing manual paper handling and physical storage, which in turn will support the Authority's Locations strategy.

4.1.2. The Authority requires the Supplier to provide a digital mailroom that will:

(a) capture a digital image;

(b) automatically index and classify mail items for routing to the Authority's workflow systems;

(c) provide data extraction for manual and automated processing by the authority;

(d) capture digital images to an evidential standard for presentation in a court of law;

(e) provide digital and physical exception handling processes;

(f) manage physical and digital mail destruction in line with the Authority's retention policies;

(g) provide full e2e traceability of all post items received from receipt to destruction (digital and physical).

4.1.3. The Authority has engaged the Supplier to provide an outcome-based service, as far as possible agnostic to technology, and therefore is not looking to be tied into a product set that is not easily portable or capable of exit and transfer to other technologies and/or providers at the end of the Contract.

4.1.4. The timely processing and digitisation of mail is a critical element of the Authority's overall Customer service levels which are measured through indicators, some of which are made visible to Ministers via No.10 Transparency Reporting.

4.1.5. The Supplier understands that it is crucial that Input Services continue to be delivered to the Authority without any interruption during and after the Transition period, and the Supplier shall assist the Authority to this end.

4.2. DIGITISATION OF NON-STRUCTURED MAIL - LETTERS / FORMS

4.2.1 The Supplier shall create digital images that are integrated into the Authority's workflow system the Digital Mail Service ("DMS"), of approximately 700 workflow queues for manual and automated processing. This process also provides exception handling for a small additional volume of mail items.

4.2.2 The Supplier shall receive paper-based mail, printed and handwritten, direct via the Authority's postal supplier(s):

(a) Royal Mail Retail - delivering post mailed to C100 BSI addresses direct from the customer including tracked mail (Special/recorded) minimally twice per Working Day;

(b) the Authority's Courier Supplier - delivering post collected from Government offices and third-party suppliers.

4.3. RECEIPT OF MAIL

4.3.1 All deliveries must be received into the supplier's premises and signed for following the individual postal provider's receipt process with each delivery allocated a unique reference that enables tracking of all associated work.

4.3.2 The Supplier shall keep the Authority's mail items secure and segregated from all other material with only individuals approved by the Authority having access to them.

4.3.3 The Supplier shall carry out pre-sort mail checks and any mail delivered in error, e.g., not addressed to the Authority, shall be returned to Royal Mail at the next delivery.

4.3.4 All mail will be pre-sorted into BSI addresses by Royal Mail prior to delivery to the Supplier.

4.3.5 The Supplier shall manage and process all post received in post receipt date order.

4.3.6 The recorded date of receipt is the date the post is received by the Supplier unless indicated otherwise via a batch header from the Authority.

4.4. BATCH HEADERS

4.4.1 A Batch Header is a template used by the Authority as a front sheet when sending items for scanning. The header is completed by the Authority and provides scanning instruction to the Supplier (for example, how and where the item needs to be scanned, date of receipt, etc.). The header detail will be agreed between the Authority and the Supplier to ensure that the Authority provides enough information for the Supplier to accurately scan the documents to the correct structure. **REDACTED**

4.4.2 At the time of Contract signing this form is generated digitally through a Supplier portal to support traceability.

4.5. TRACEABILITY

4.5.1 The Supplier must provide an electronic process where all mail items can be tracked throughout their full end-to-end journey (receipt to destruction) and are uniquely identifiable. This must include but is not limited to:

(a) logging the date and time of the delivery and allocation of a unique delivery reference that can be used to track all work that stems from that delivery;

(b) all envelope contents to remain together and linked to the envelope, the batch and the delivery from which it came;

(c) each envelope to be allocated a unique ENVA reference (**REDACTED**);

(d) a unique scan reference for mail items within each envelope following the envelope splitting guidance for each BSI (**REDACTED**);

(i) where the mail items within an envelope are split and scanned as separate mail items, they must be allocated individual unique scan references, but the documents annotated in a way that the Authority can identify that there are further envelope contents. For example: a sticker showing NEWDOC;

(e) the ENVA reference and scan reference must form part of the metadata transferred to the Authority with the digital image;

(f) all Royal Mail Special and Recorded Delivery tracking references;

(g) valuable Items must be scanned prior to return to the customer and the image clearly annotated with a unique VI number (**REDACTED**) A full audit trail of where the Valuable Items are returned must also be maintained;

(h) logging of all exceptions returned to the Authority or sent on to a third party including a tracking process and manifest that enables the receiver to acknowledge receipt.

4.6. MAIL PREPARATION

4.6.1 The Supplier shall identify all BSI addresses for the Non-structured service, open, sort, record receipt and prepare mail for digitisation as defined for each BSI address.

4.6.2 The Supplier shall respect the following rules to maintain the integrity of the received mail:

(a) mail items received for each BSI must be kept together. Items from one batch cannot be mixed with items from another;

(b) opened mail should be placed back in the batch in the same order as they were originally in the batch;

(c) the contents of every envelope must always be handled in the order in which they were taken out of the envelope unless specified as otherwise by The Authority;

(d) items from the same envelope must be kept together;

(e) each sheet of paper Must be scanned separately in Duplex;

(f) handling of non-scannable items, valuables and exceptions must conform to the processes prescribed in the document (**REDACTED**).

4.6.3 Within specific BSI addresses some forms must be out sorted and then routed to pre-defined queues to support automation by the Authority:

(a) pre-defined Self-Assessment forms are also subject to a data extraction process to enable the Authority to automatically log receipt and inhibit non-filing penalties The data is passed to the Authority via secure link for processing through the Authority's HODs;

(b) The Supplier must:

(i) have the ability to connect to SDES, DES and IF as outlined in (**REDACTED**); and

(ii) know the file format and structure of the files that will be sent. Specifically, the Supplier shall provide a time critical daily file in .csv format for the purposes of preventing penalty notices from being issued inappropriately. For post items where data could not be extracted to enable automatic logging, a daily 'not logged' file shall be shared with the Authority for manual logging. These forms then continue through the Non-structured process to be scanned and transferred to the Authority to land in DMS.

4.6.4 The Supplier must manage timely and safe return of specified Valuable Items directly to Customers after digitisation, using the agreed postal arrangement(s) and the Address rules provided by the Authority:

(a) for a current list of items classified as 'valuable' (**REDACTED**) This will be updated as required by the Authority;

(b) where the address isn't obvious the whole envelope shall be returned to the Authority post scan as an exception;

(c) valuable items must be returned to the customer in an envelope and with a compliment slip and addressed as per the Authority's rules. All consumables shall be provided by the Authority;

(d) all valuable items will be collected daily by the Authority's downstream access provider.

4.6.5 The Supplier shall provide a reconcilable cheque handling process to integrate with that of the Authority's cheque clearing provider. **REDACTED**:

(a) where a cheque forms part of the mail item the whole envelope is currently extracted;

(b) the whole envelope including all contents is then distributed to different Locations to be specified by the Authority via the Authority's dedicated van provided by the Network courier;

(c) all cheques sent onto the cheque clearing provider and/or the Authority must be accompanied both digitally and physically by a manifest to support traceability. The template must be developed/generated by the Supplier in agreement with the Authority.

4.7 EXCEPTIONS

4.7.1 The Supplier must extract pre scan exceptions. These mail items are a mixture of unscannable items (for example USB stick) and exceptions identified by the Authority to be returned as paper. For a current list of items classified as 'exceptions' (**REDACTED**) This will be updated as required by the Authority.

4.7.2 The Supplier shall return any physical exceptions to the Authority's Locations as per the business rules. This will include a manifest detailing the mail items returned to ensure traceability and reconciliation.

4.7.3 The Authority requires the Supplier to return post items to the customer where there is incomplete form completion across some of its Queue Structures, and the Supplier shall do so.

4.7.4 The Authority will provide all consumables including the appropriate correspondence to include with the returned documents.

4.8 SCANNING

4.8.1 The Supplier shall correctly index and optimise automatic queue Classification and correct routing of all mail items (including handprint and handwritten/cursive), with minimal manual intervention through the use of the keyword structures attached to each of the BSI postal addresses to route mail items to the correct queues and pick up and record key data used to form the xml data (metadata) passed to the Authority.

4.8.2 The Supplier shall provide digitised PDF/A image/xml data to the Authority via a secure electronic link, for ingestion into the Authority's workflow system (DMS) and digital repository.

4.8.3 The Supplier shall meet the Interface requirements and specifications as set out in Annex 2.02 Input Services Technical documents.

4.8.4 **REDACTED**.

4.8.5 The Supplier shall delete images and handover physical documents to the Authority's secure waste management provider at the end of the retention period:

(a) the waste management provider will collect material to be destroyed from the scanning Supplier's Premises;

(b) frequency of collection will depend on the agreement with the Supplier, depending on the ability to store and other contingent factors.

4.9 RESCAN AND HARDCOPY RETRIEVAL

4.9.1 The Supplier shall fulfil daily re-scan and physical document retrieval requests.

4.9.2 The Supplier shall provide a digital process where these requests can be made by the Authority.

4.9.3 The Authority reserves the right to request a rescan within the retention period timescales where the item has not been scanned correctly i.e., overlap, mixed customers, and:

(a) any request by the Authority for re-scan based on Supplier error must not be chargeable, and the Supplier must not charge the Authority for this;

(b) when a re-scan is requested, the Supplier shall investigate the issue and advise whether a re-scan is possible or beneficial (the original image may be the best possible quality);

(c) if a re-scan is necessary then the Supplier shall retrieve the physical document, scan and re-export them using the original document reference(s);

(d) hard copy retrievals must be returned to agreed locations via the Authority postal courier network (addresses provided by the Authority). Any hardcopy retrievals requested are returned as the whole envelope contents.

4.10 DIGITALISATION OF STRUCTURED MAIL-INPUT SERVICES

4.10.1 The Supplier shall be responsible for the digitisation, exception handling and capture of handprint data from Structured Mail including continuation sheets and schedules for integration into the Authority's back-end transactional processing systems. The Supplier shall also be responsible for the digitisation of mail items for integration into the Authority's Caseflow system.

4.10.2 The Supplier shall receive paper-based mail comprising of Handprint Forms, together with continuation sheets/schedules and records relating to Compliance enquiries. These will be sent directly to the Supplier via BSI address or from the Authority under cover of a batch header via the Authority's approved postal providers:

(a) for some form types the Authority requires the ability to send schedules to the Supplier digitally, and the Supplier shall have capability to receive these schedules;

(b) the specific requirements will be agreed between the Authority and the Supplier.

4.10.3 All postal deliveries must be handled in the same manner as detailed in the Non-structured route.

4.10.4 The Supplier shall provide reconcilable pre and post scan exception processes (physical and online) with any physical exceptions returned to the Authority as detailed in the Non-structured route.

4.10.5 The Supplier shall provide a digital decision-making process for mail items not meeting the Structured rules. All such exceptions will be processed via an online portal, this must include but is not limited to, the ability to:

(a) route online digital exceptions back to the supplier for processing;

(b) transfer to the Authority via the non-structured route into the case management service as either a live or closed work item;

(c) return to the customer via the Authority's downstream access provider;

(d) return the original documents to the Authority via the Authority's courier service.

4.11 **TRACEABILITY**

4.11.1 The Supplier shall provide an electronic process where all mail items can be tracked throughout their full end-to-end journey (receipt to destruction) and are uniquely identifiable. This must include but is not limited to:

(a) logging the date and time of the delivery and allocation of a unique delivery reference that can be used to track all work that stems from that delivery;

(b) all envelope contents to remain together and linked to the envelope, the batch and the delivery from which it came;

(c) each envelope to be allocated a unique ENVA reference (**REDACTED**);

(d) a unique scan reference for mail items within each envelope following the envelope splitting guidance (**REDACTED**);

(i) where applicable the ENVA reference and the scan reference must form part of the Metadata transferred to the Authority with the digital image. All Royal Mail Special and recorded Delivery tracking references;

(ii) valuable Items must be scanned prior to return to the customer and the image clearly annotated with a unique VI reference (**REDACTED**). A full audit trail of where the valuable items are returned must also be maintained;

(iii) logging of all exceptions returned to the Authority or sent to a third party through a tracking process and manifest that enables the receiver to acknowledge receipt.

4.12 **MAIL PREPARATION**

4.12.1 The supplier shall identify all BSI addresses for the Structured service, open, sort, record receipt and prepare for digitisation as defined for each BSI address.

4.12.2 The rules to maintain the integrity of the received mail must be followed as per the Non-structured Mail route.

4.12.3 The Supplier shall process Valuable Items as described in the Non-structured Mail route.

4.12.4 The Supplier shall follow the cheque handling process as described in the Non-structured Mail route.

4.13 EXCEPTIONS

4.13.1 The Supplier shall provide reconcilable pre and post scan exception processes (physical and online). The Supplier shall return any physical exceptions to the Authority as per the Non-structured Mail process.

4.13.2 The Supplier shall provide a digital decision-making process for mail items not meeting the Structured business rules/minimum data sets. All such exceptions shall be processed via an online portal, which must include but is not limited to, the ability to:

(a) route online digital exceptions back to the supplier for processing;

(b) transfer to the Authority via the Non-structured Mail route into the case management service as either a live or closed work item;

(c) return the original documents to the Authority via the Authority's courier service;

(d) return to the customer via the Authority's downstream access provider.

4.14 SCANNING

4.14.1 The Supplier shall scan mail and intelligently capture the correct data recognising both machine and handprint and applying both validation and business rules. Bank details and addresses are validated for specific forms.

4.14.2 Data is to be extracted from the image in accordance with the Business rules with verification and correction carried out as required:

(a) data fields to be extracted are pre-defined by the Authority. Verification is to ensure data extraction is correct and correction as applicable. No other correction is required, and data extracted must match the image;

(b) for pre-defined BSI addresses files are text searchable in PDF/A format;

(c) the Authority will provide software licences (**REDACTED**) to the Supplier to enable bank account details validation for some Structured forms.

4.14.3 Any exceptions not matching business rules/minimum data sets are managed through the digital portal by the Authority.

4.14.4 Any changes made by the Authority to the form's templates must be tested by the Supplier and changes made to extraction rules as appropriate. These changes may be ad-hoc or yearly, dependant on form type.

4.14.5 Caseflow scanning must conform to BS10008.

4.14.6 The document image should be stored in an image repository, archived as per the Authority's retention requirements and made available for retrieval.

4.14.7 The Supplier shall provide digitised xml data via the Authority's approved inbound connectivity pathways, including DES, SDES and IF, for seamless integration and downstream transactional processing by the Authority's IT systems:

(a) the Supplier shall provide a log file and .csv file for each structured csv file passed to the Authority;

(b) for VAT100 files the Authority requires a JSON file to be generated and passed to the Authority each time a file is created for integration into our systems;

(c) for Caseflow the Authority requires a text searchable PDF;

(d) specifically, the Supplier shall provide a time critical daily log file for the Tax Credit work stream, to enable reconciliation with XML data in time for scheduled downstream transactional processing;

(e) the Supplier shall provide a time critical daily log file at 4pm each day detailing all xml files that have been passed to the Authority by the Supplier throughout the day;

(f) the Supplier shall provide digitised PDF/A image/sub-set XML data for ingestion into the Authority's digital repositories.

4.14.8 **REDACTED**).

4.14.9 The Supplier shall delete images and handover physical documents to the Authority's secure waste management provider after the retention period as described in the Non-structured Mail route.

4.15 RESCAN AND HARDCOPY RETRIEVALS

4.15.1 The Supplier shall fulfil rescan and hardcopy retrievals as per the Non-structured Mail route.

4.16 EVIDENTIAL SCANNING

4.16.1 **REDACTED**.

4.17 **BACK SCANNING**

4.17.1 The Back Scanning of Mail Items for Integration into the Authority's Digital Mail Service as a Closed Work Item.

4.17.2 The Supplier shall receive, scan and create an accurate image of Customer information. These mail items will be delivered to the Supplier with a batch header via the Authority's dedicated network courier.

4.17.3 Back scan items are received regularly for some Queue Structures but there will be instances where the Authority requires the Supplier to scan volumes of archived material. In these instances, the Authority will agree appropriate performance measures based on the content with the Supplier and:

(a) the Supplier shall ensure each item is uniquely identifiable throughout the full end-to-end process;

(b) the Supplier shall record receipt of the mail items and prepare for digitisation as per the Authorities instructions;

(c) the Supplier shall Index and scan each item;

(i) each file shall be split by customer unless advised differently by the Authority;

(ii) each file will be given an ENVA number with any subsequent correspondence linked within that file scanned as an individual PDF and linked to the original ENVA;

(iii) the Authority reserves the right to request bespoke indexing based on the consignment to be agreed in advance with the Supplier;

(iv) the Authority requires these items to be annotated by the Supplier within the metadata to advise the Authority that these should be ingested to the Digital Mail Service as a closed item.

(d) the Supplier shall supply digitised PDF image/xml data to the Authority via secure electronic link as per the Non-structured route for ingestion into the Authority's Digital Mail Service;

(e) the Supplier shall retain the physical/digital documents as per the retention period (50 Working Days) unless returned to the Authority as requested. At the end of the retention period the Supplier shall delete the images and handover any physical documents to the Authority's secure waste management provider.

4.18 SCANNING/DATA EXTRACTION

4.18.1 The Scanning and Extraction of Data from Specified Mail Items for Robotic or Other Automated Processing by the Authority Currently this supports mail returned via Royal Mail's Returned Letter Service ("RLS"). This service must provide the Authority with either a digital image only or a digital image together with a data extract for integration with the Authority's robotic service or other case management services.

4.18.2 The Supplier shall receive mail items via the Authority's postal providers:

(a) the Supplier must open, sort and prepare mail for digitisation in line with the Authority's instruction as per the Non-structured & Structured rules;

(b) the Supplier shall specifically provide exception handling (for cheques and Valuable Items identified during preparation) as per the Non-structured & Structured rules;

(c) the Supplier must out sort pre-defined form types. (prior to the award of the Contract, 145 form types) and follow differentiated processes for each of the business streams (Personal Tax ("PT")/Corporation Tax ("CT")/Debt Management ("DM")/Corporate Finance ("CF")) For PT/CT/DM the Supplier must scan, classify, and intelligently capture data (from the front sheet only and as defined by the Authority);

(i) for PT/CT/DM, for items NOT meeting business rules, the Supplier must scan the items to specific DMS queues including indexing data. The envelope reference will be indexed as an ENVR number and 8 numeric digits (the ENVA is changed to ENVR to denote RLS). The scan ref will be RL followed by 10 integers;

(ii) for CF the Supplier must scan and classify these to a pre-defined DMS queue and allocate an ENVA number;

(iii) the Supplier must provide digitised PDF image/xml, CSV or JSON data and associated metadata to the Authority via hard drive and secure courier. The Authority is moving to electronic transfer of this data from Supplier to Authority, via one of the Authority's approved inbound connectivity pathways, including SDES and IF, which may or may not be completed prior to any transition;

(d) For the remaining items (not pre-defined) the Supplier must scan through the Non-structured line (page one only) and classify to a pre-defined DMS queue. These items will require a ENVR reference to denote RLS.

4.18.3 The Supplier must, except for mail items processed as an exception (Valuable items or cheques), arrange for the mail items to be included in the next collection of waste for secure destruction by the Authority's waste management provider (unlike other services, the Supplier must retain the digital image for 50 Working Days; physical items must be destroyed straightaway).

4.19 **COOPERATION**

4.19.1 The Supplier shall work closely with the Authority's internal teams and external Suppliers.

4.19.2 The Supplier shall liaise with the e2e supply chain and includes but is not limited to:

(a) Royal Mail Retail;

(b) Down Stream Access Provider;

(c) dedicated network courier;

(d) secure Waste Management provider;

(e) secure courier provider.

4.19.3 The Supplier must engage with all external suppliers and the Authority to agree, setup and manage implementation and change activities including account set ups. (The frequency of collections and deliveries by external providers are currently daily (Monday - Friday) unless specified otherwise).

4.20 **STORAGE REQUIREMENTS**

4.20.1 In relation to the environment where HMRC property is stored by the Supplier, the storage areas must be designed to meet the following storage conditions to ensure no deterioration/damage to the quality of goods:

(a) meet the requirements of the national Health and Safety at Work Legislation;
(b) meet suitable storage conditions to ensure no deterioration/damage to the quality of goods;
(c) be secure with only access granted to authorised personnel;
(d) kept in good repair.

4.20.2 There must be provisions to check, monitor, and record the above parameters.

4.21 SUPPORT FOR COLLEAGUES WITHIN THE AUTHORITY

4.21.1 The Supplier shall support colleagues within the Authority. For example, this could be to help colleagues understand how the scanning services work, or to enable a product or service to be quality checked.

4.21.2 The Supplier shall provide support including, but not limited to:

(a) hosting onsite visits and tours of the scanning services;

(b) information packs about the scanning services, including size and scale, equipment used, facilities and environment;

(c) virtual site/services tour.

4.22 **ONLINE PORTAL-INPUT SERVICES**

4.22.1 The Supplier shall provide a digital platform that will perform, but is not limited to, the following functions for the Authority:

(a) rescan and hardcopy retrieval requests;

(b) view/search all scanned documents during the period of retention, to include capability to search on a reference number (including special and recorded delivery references);

(c) view MI as detailed in the MI section for real time information and historical reporting, with the ability to configure, customise and export the reports in an editable format;

(d) the ability to restrict and manage user access;

(e) manage exceptions from UI drop down options. For exceptions generated from the Structured and non-structured Mail process, the options must include but are not limited to:

(i) why the mail item is an exception;

(ii) request to return to Structured Mail process for processing;

(iii) capability to forward to Non-Structured Mail process (e.g., letter received with Structured form);

(iv) ability to manage Valuable Items;

(v) prioritise and route online digital exceptions back to the supplier for processing;

(vi) transfer to the Authority via the Non-structured route into the case management service as either a live or closed work item;

(vii) return to the customer and closure;

(viii)return the original documents to the Authority;

(ix) the Authority reserves the right to request further options on an ad-hoc basis.

4.22.2 The Supplier shall ensure that the functionality enables a user to see if another user is working on the item, without having to select and open it.

4.22.3 The Supplier shall ensure that the notes from the Supplier's portal can be exported with any mail item for ingestion to DMS.

4.22.4 The Supplier shall ensure that the functionality enables a user to work through multiple items at the same time without having to select each one individually.

4.22.5 The Supplier shall ensure that the functionality enables the Authority to override default activity (e.g., stop the automatic issue of a compliment slip).

4.22.6 The portal must be available 24/7/365, with full customer support being available from 07:00 to 20:00 during Working Days.

4.22.7 Ensure any routine maintenance takes place outside of standard operating hours (07:00 – 20:00 during the Working Days) where possible and must be non-disruptive.

4.22.8 The Authority needs to be notified about any such routine maintenance within a specified and agreed time-frame, a minimum of one calendar month in advance and:

(a) portal response time of three (3) seconds or less 95% of the time;

(b) the ability to hold a minimum of 600 users and 40% concurrency;

(c) the portal will time out users that have been inactive for 30 minutes;

(d) provide user logs that are fully auditable, and the Authority must have access to these;

(e) the ability to ingest/cut over all data held on the incumbent Supplier’s portal;

(f) the Supplier shall provide training, along with support mechanisms to consolidate learning, to the Authority, ensuring users can use the portal effectively. The Authority requires the ability to utilise the training material internally as required;

(g) the Supplier shall provide a user-friendly guide for the portal;

(i) the portal must meet accessibility standards.

4.23 QUALITY

4.23.1 The Supplier must scan all documents at 300 DPI, unless exceptionally a higher or lower resolution is requested by the Authority.

4.23.2 The Supplier must ensure that there is no image degradation, by ensuring an optimum level image is created based on the respective DPI.

4.23.3 The Supplier must ensure that images are scanned the right way up:

(a) the Supplier must provide scanned images in black and white as the default, but, exceptionally, across the various service offerings to provide an image in greyscale or colour. This does not apply to Evidential Scanning;

(b) for Evidential Scanning, this exception is covered in more detail in (see paragraph 4.16, Evidential Scanning).

4.23.4 The Supplier is expected to perform quality checks across the separate services, some of which are included under the service headings. As an example, this will include:

(a) ensuring full traceability of items received by the Supplier with particular attention paid to Valuable items, cheques and exceptions;

(b) optimal indexing and classification of postal items;

(c) optimal recording of Customer Identifiers;

(d) validation of correct data extraction;

(e) sample check of true likeness to original image.

4.24 MANAGEMENT INFORMATION (MI)

4.24.1 The Supplier must provide real time and historical reports to the Authority in a digital format with the capability to provide offline as well where necessary, as part of the online portal provision. The contents of the reports will be agreed by both Supplier and Authority and should have the flexibility to evolve with the Authority's requirements over the lifetime of the contract.

4.24.2 The reports must cover all services and products and will consist of, but are not limited to:

(a) traceability of E2E customer journeys and supporting MI;

(b) forecasting data;

(c) receipt data broken down to service line:

(i) non-structured split by BSI, Queue Structure and queue;

(ii) structured split by BSI;

(iii) back scanning split by Queue Structure and queue;

(iv) evidential as detailed in the service line requirements:

A. volumes of scanned items shown as volume of docs and images;

B. for RLS data extraction the split of items that have met/not met robotics requirements and those not in scope;

C. on hand data/SLA information. Service Performance against the SLAs described in Schedule 2.2 (Performance Levels);

D. daily volume of exceptions, cheques and valuable items;

E. daily volume of courier items and BSI envelopes received by the Supplier by Queue Structure;

F. volumes across the end-to-end process (received, on hand, processing milestones) – to help inform resource planning/channel shift (including blending of telephony and post) across all service lines with the ability to drill down to queue data;

G. data on which to perform analytics – to help understand, for example, trends, mail Classification, BSI usage, volume of retrievals and re-scans, volume of cheques received, volume of valuable items;

H. a monthly cost breakdown of charges for each rate card entry, which will form the basis for monthly invoicing and invoice reconciliation by the Authority;

I. accurate, complete MI and traceability, and performance measures around this, for all products.

4.24.3 The Supplier shall provide a contact who will attend regular and ad-hoc checkpoint calls to keep the Authority informed of any issues with quality, processes and identify any risks to delivery, ensuring these are resolved promptly.

4.24.4 The Supplier shall attend review meetings as specified in Schedule 8.1(*Governance*).

4.24.5 Where services and products are provided by a Sub-contractor relationship, the Authority requires the same level of MI from the Supplier, and the Supplier shall provide this.

4.24.6 For Evidential Scanning, the Supplier shall also provide any ad-hoc reports requested for specified consignments. In addition to the weekly update calls and the SLA/progress details, if at any time more detailed reports on a case are needed, or problems encountered with it, the Supplier shall update the Authority over and above the information being shown on the weekly updates.

4.25 CHANGE REQUEST AND TESTING

4.25.1 As well as the transitional testing requirements, on a regular basis the Authority will require changes to any of the services detailed above. The Supplier must provide a test environment for each service, full end to end testing for any change with the ability to roll back as applicable, full happy and sad path testing, the ability to run multiple changes in parallel and the ability to test live mail items. The Authority will work with the Supplier to develop and agree a test plan for each change at the time.

4.25.2 The Supplier must inform the Authority two months in advance if they wish to implement a change freeze. The Authority reserves the right to either accept or reject this request. The Authority may reject the request if there is an urgent change which is required to be implemented during the period for example: legislation changes.

4.25.3 All Change Requests should be managed in line with the procedures set out in Schedule 8.3 (Change Control).

4.25.4 There are 4 types of change requests that may occur:

(a) contract change requests (see Schedule 8.3 (*Change Control Procedure*));

(b) operational change requests;

(c) IT Change Requests; and

(d) statement of work will be used on projects that do not sit under the 1, 2 or 3 (**REDACTED**).

4.26 DISASTER RECOVERY

4.26.1 The Authority requires a minimum of dual site processing.

4.26.2 The Supplier needs to have inter-site operability, with active flex and disaster recovery.

4.26.3 The Supplier shall have reliable and robust disaster recovery capabilities to ensure no interruption to service in the event of a data centre outage. This shall include the use of multiple geographically resilient datacentres and/or high availability patterns where cloud infrastructure is used.

4.26.4 In a disaster recovery situation, the Supplier must be able to stand up all services by the next Working Day.

4.27 SUPPORT

4.27.1 The Supplier must provide UK-based support. A dedicated Helpdesk (telephone) and specific contact points (email)/escalation routes are required to resolve customer issues during the hours Monday – Friday 07:00 – 20:00, as a minimum.

4.27.2 The Supplier shall provide support for issue resolution, regardless of whether the root cause lays with the Supplier, Authority, or both.

4.27.3 A dedicated Supplier service manager must be provided to facilitate business as usual activities, general queries, incident management, change activities and regular service reviews, including performance review.

4.28 INCIDENT MANAGEMENT

4.28.1 An Incident is anything which causes an interruption or a reduction in the quality of the service and is not limited to IT.

4.28.2 Incidents may occur outside of the Authority's working hours and the Supplier must provide support at the time should this be identified outside of those hours. The Authority and Supplier must share named individuals and contact details for such events.

4.28.3 The Authority's priority levels are outlined below, the Supplier's incident management procedures must meet and align with these timelines and guidelines as a minimum.

4.28.4 The Supplier must report any incident when it is identified. The response time is the target time from the time an incident is identified to the time an initial response is sent back to the Authority.

4.28.5 The resolution time is the maximum time that the Authority expects the Supplier to restore the service to a level acceptable to the Authority. The resolution time is calculated by a "stop the clock" approach whereby the clock is only paused or suspended when a query or question is directed to the Authority. This ensures the total time taken for resolution is accurately calculated. The Authority reserves the right to work with the Supplier flexibly to adjust the resolution time dependant on the nature of the incident.

Priority Level	Business Impact Summary	Response time	Resolution Time
Critical – P1	A complete outage where the Service cannot be accessed, affecting more than 75% of service or an incident that has a serious or reputational impact to the Authority	15 Minutes	4 Service hours
Major – P2	Service affecting or partial outage, including intermittent failures, affecting more than 50% of service or an incident that has a significant impact to the Authority	1 Hour	8 Service Hours
Minor – P3	Minor Service impact on system functions or affecting only single users. No direct impact on full service availability, or an incident that has minor impact to the Authority	6 Hours	2 Service Days
Low – P4	Low impact on the Service or system functions.	1 Business Day	3 Service Days
Low – P5	Low impact issue with single user or output.	1 Business Day	5 Service Days

4.29 INTEGRATION

4.29.1 The Supplier shall provide and configure any hardware and/or software needed to integrate and be fully compatible with the Authority's systems.

4.29.2 The Supplier must be able to connect to the Authority's Secure Data Exchange Service (SDES) via an agreed file transfer protocol.

4.29.3 The Supplier must be able to:

(a) transfer files via FTPS;

(b) support TLS 1.2 encrypted connection (as a minimum);

(c) support one way authentication.

4.29.4 The Supplier shall have a specific static IP address range from which its FTPS software will connect to the Authority. The IP address range must include two addresses each for Test connection and Production Connection: one for the active connection and the other for the failover. (Specific IP Address details, Port numbers and FTP Command sequences will be shared with the successful Supplier during transition).

4.29.5 The Supplier must be able to connect to the Authority's Data Exchange Service via VPN connection:

(a) data traffic from the Supplier shall pass through the VPN and the Authority's Networks' firewalls;

(b) data traffic from the Authority must pass through the VPN and the Supplier's firewalls into their internal networks (Specific IP Address details, Port numbers and other technical details will be shared with the successful Supplier during transition).

4.29.6 The services within the Supplier's solution platform utilise lightweight protocols (e.g., RESTful APIs) based on open standards.

4.29.7 The Supplier's digital products must support the use of OAuth (preferred) or SAML integration with the Authority's AzureAD for user authentication.

4.30 **UPGRADES**

4.30.1 The Supplier shall ensure any routine maintenance takes place outside of standard operating hours (07:00 – 20:00 Monday – Friday and 07:00 – 1600 on Saturday) and must be non-disruptive.

4.30.2 Any software updates must be planned in advance and agreed by the Authority. All planned maintenance must adhere to the Authority’s change management policies (CAB approval) and

be submitted with appropriate forward notice period dependent upon the impact of any service outages along with details of an actionable regression plan.

4.30.3 In the event of an unsuccessful update, consultation shall be within 1 hour and agree remediation activities to restore service.

4.31 SECURITY

4.31.1 Data must be encrypted at rest using unbroken algorithms. At a minimum, this will be at a minimum AES256 or equivalent.

4.31.2 Where required, data must be encrypted in transit using unbroken algorithms. At a minimum, this will be at least TLS 1.2 (Transport Layer Security) for web traffic.

4.31.3 The Supplier should be able to receive reconciliation/receipt messages from the Authority via API.

4.31.4 All user actions and automated system actions be logged and be auditable to ensure security is not compromised.

4.31.5 For Evidential material, the Supplier must provide integrity verification for electronic files passed to the Authority, using methods and Algorithms agreed with the Authority:

(a) at a minimum, SHA256 or equivalent.

4.31.6 Prior to Contract go-live, the Authority will conduct security on-site reviews to ensure the Supplier's physical estate and processes meet the requirements.

4.32 DATA

4.32.1 All data should reside in the UK, including disaster recovery and failover scenarios.

4.32.2 The Supplier shall package transfer these documents as ZIP archives to the Authority.

4.32.3 Documents to be imported must be in the stipulated XML format.

4.32.4 Encoded documents must be marked as such within the XML metadata.

4.32.5 Native format documents must be specified in the Control List file for the batch.

4.32.6 A Control List file in the stipulated format must be available for each batch import.

4.32.7 For Evidential Scanning, the Supplier must:

(a) create a Batch Interface File that comprises of zipped scanned evidence documents;

(b) generate an associated metadata file with the manifest section fully populated for every scanned evidence file present in the zipped Batch Interface File.

4.32.8 Images must be provided in the agreed data format and the Supplier must move with the current industry standards, i.e., PDF/A rather than PDF. (The Authority will provide instructions to the Supplier for which file types are required for different document types).

4.32.9 Metadata must be provided in the agreed data formats as agreed with the Authority, and the Supplier must move with the current industry standards.

4.32.10 The Supplier must be able to provide data in a format dependent on the end application including, but not limited to:

(a) CSV;

(b) PDF/A;

(c) XML;

(d) JPEG;

(e) JSON.

4.32.11 Documents are to be embedded/encoded within the XML created for each document.

4.32.12 The structure of document imports must be as determined by the Authority.

4.32.13 The Supplier must provide files with sizes according to specifications agreed with the Authority.

4.32.14 If a batch is bigger than the agreed file specification, the Supplier must be able to split the batch while still keeping the integrity and lineage of the overall file. For example, in the case of Evidential Scanning, the Batch Interface File's maximum size will be 4 gigabytes. Since each Batch Interface file will be comprised of a single consignment (which is all the material for a particular case), if the delivered file is more than 4gb, it must be split into files not greater than 4gb, and the various smaller files should be identifiable via custom naming schemes at a minimum.

4.32.15 Information Lifecycle Management policies must be implementable for all data retained within the Supplier's digital platforms.

4.33 MULTI-LINGUAL COMMUNICATIONS

4.33.1 The Service must be able to receive multilingual communications. Currently these are managed through the keyword recognition process for queue classification and there is a requirement to recognise non-standard characters.

4.34 FUTURE AMBITIONS

4.34.1 The Authority would like to consider service improvements to increase the XML metadata types transferred and ingested to DMS for the non-structured Mail process. **REDACTED**.

4.34.2 The Authority may require a service to scan and receive envelopes digitally to support downstream processing, in particular RLS.

4.34.3 To support the Authority's location strategy to reduce on site storage capacity, there may be a requirement to scan historical documents. These documents may be degraded and on non-standard paper.

4.34.4 The Authority is currently exploring the ability to provide assurance to customers on receipt of whitemail via mobile messaging.

4.34.5 The Authority is currently exploring the use of barcodes (that are attributed to all incoming work to track the work item through the supplier). **REDACTED**.

4.34.6 Improved E2E process to deliver scanned images that enable the Authority to increase automation of document processing, this might include increased data extraction with conversion to JSON files to enable the Authority to exploit AI.

4.34.7 The Authority is considering an enhancement to its downstream case flow management system (DMS) that would support text searchable PDFs for all items and the ability to search on form type. This would require the ability for form type to be identified at scanning and passed to the Authority as part of the metadata.

4.34.8 Prior to this Contract, the Authority does not routinely scan SCR post through suppliers. There is a requirement to do this which may require bespoke arrangements which may or may not be delivered prior to Transition.

4.34.9 **REDACTED**. For a number of forms in the Structured service the Authority may choose to improve the process by moving all data validation to The Authority requiring the Supplier to use data extraction only.

4.34.10 In the future the Authority may require the PDFs to be text searchable across all Scanning services. This is currently done for Evidential and Case-flow.

4.34.11 Pending the introduction of the Authority's own in-house capability (change not yet commissioned), the Authority may wish the Supplier to receive or access communications sent to the Authority by email and absorb them into the Digitisation of non-structured Mail process described in Service Offering 1) (See Annex 2.01 MSOG).

4.34.12 During the lifetime of this contract the Authority may look to develop a solution for inbound post from the Valuation Office. The full requirements will be scoped at the point that the Authority wishes to take this forward.

5 PART C: Description of Email and Mobile Messaging Services

5.1 INTRODUCTION TO EMAIL AND MOBILE MESSAGING SERVICES

5.1.1 The Authority has engaged the Supplier to provide an Email and Mobile Messaging delivery platform which will issue digital communications to its customers. The Supplier shall provide comprehensive end-to-end customer communication services that support the Authority's operating model, and specifically the increased use of digital services.

5.1.2 The Authority anticipates an increase in Email and Mobile Messaging communications, and expansion into wider and emerging mobile messaging channels, as it looks to achieve our digital transformation ambition.

5.2 SERVICE DESCRIPTION

5.2.1 The Supplier shall provide a Service to compose, schedule and/or deploy Email and Mobile Messaging communications. This must be low code/no code and user intuitive.

5.2.2 Email communications include Marketing Campaigns and Transactional Email communications.

5.2.3 Mobile Messaging communications include SMS, Rich Communication Services ("RCS"), Apple Messages for Business and other such current and emerging communication channels.

5.2.4 The Supplier shall provide:

(a) the Service 24/7/365;

(b) an integrated datastore (Paragraph 5.9) which enables defined Authority users to access and maintain all customer data;

(c) a hosted Customer Preference Portal (Paragraph 5.11) for customers to sign up to manage and unsubscribe from email topic preferences;

(d) the ability to send out multilingual communications, currently English and Welsh. This may be expanded in the future;

(e) the ability to create multiple segmentations, groups and sub-groups which breakdown campaigns and associated costs;

(f) the ability to retain and transition the Authority's current dedicated short-code for SMS and any other registered Mobile Messaging capabilities;

(g) the ability to issue communications from the Authority's multiple domains and sub-domains.

5.3 **MARKETING CAMPAIGN REQUIREMENTS**

Design and Composition

5.3.1 **REDACTED**.

5.3.2 If the use of Quadient Interactive is not implemented at the point of transition, the following are the minimum requirements for design and composition:

(a) there must be continuity of the current Email and Mobile Messaging communications style and branding;

(b) the Authority can create, amend, duplicate, maintain, archive and delete unlimited Email and Mobile Messaging templates, including a master template, without requiring technical/coding expertise (low code/no code);

(c) the ability to re-use and amend existing draft and prior sent digital communications;

(d) the ability for created templates to be stored under version control with an applicable naming convention;

(e) the ability to export templates;

(f) provide the tools and capabilities that demonstrate how Email and Mobile Messages will render on target email clients, webmail clients, desktops, mobile devices and all other applications (responsive capabilities) in advance of sending them;

(g) the ability for A/B testing;

(h) allow easy creation, automation and maintenance of customer journeys through campaign management;

(i) the ability to have personalised and/or dynamic content based on a number of provided variables including, but not limited to, sender and recipient details, message headers, greetings, text and images in content bodies, and hypertext URLs;

(j) the ability to add, format and contextualise hyperlinks, with reportable tracking available from any click-through of links;

(k) the Supplier's design process must allow for a two-stage internal quality checks prior to deployment of any campaigns;

(l) view a pre-send forecast campaign summary of volumes and associated costs for both Email and Mobile Messaging, specifically with a breakdown of message parts for Mobile Messaging;

(m) view a post-send actual deployment summary of volumes and associated costs for both Email and Mobile Messaging. Specifically with a breakdown of message parts for Mobile Messaging.

5.4 **Marketing Campaign Email specific requirements**

5.4.1 The Supplier shall provide the following requirements of the Authority:

(a) the functionality to copy and paste/import content into created email templates;

(b) the templates to be HTML5 and CSS compatible. The Authority must have support for enabling those functions and the ability to edit HTML;

(c) a central repository where global CSS styles, text styles and resources such as logos/images can be content managed and used for designing templates. To also allow global control over common resources and styles;

(d) the ability to maintain and edit text styles to quickly format the content whilst designing email templates;

(e) the composition tool to produce semantic HTML to support with improving the accessibility of emails;

(f) full email text edit functions, enabling the placement of text, text size, banners, the ability to format text, headings and the ability to store and include/update images and signature images. The design must conform to accessibility standards. In addition to meeting WCAG 2.1 AA, the Supplier shall assure the Authority that the content is tested to ensure it is usable on a wide range of assistive technologies;

(g) the ability to provide one-click links to unsubscribe from all topics, allow for temporary opt-outs, or to manage preference options (see Paragraph 5.11, Customer Preference Portal);

(h) the ability to add URL/hyperlinks to images as click-through such as Twitter/YouTube/Webinar;

(i) the ability to add anchors to email to allow the customer to easily navigate to the contents of an email.

5.5 MOBILE MESSAGING SPECIFIC REQUIREMENTS

5.5.1 The Supplier must provide the functionality to allow the Authority to:

(a) preview messages with their character count before sending to show how many message parts the message will be split across;

(b) be able to set character-sets for SMS on demand, for example Unicode.

5.6 SCHEDULING AND DEPLOYMENT

5.6.1 The Authority requires the solution to have:

(a) the ability to issue one-time or recurring campaigns on a live or pre-scheduled basis;

(b) the ability to issue event triggered communications via API. Some communications will be triggered through the Authority's other suppliers;

(c) the ability to issue multiple campaigns, of fluctuating volumes, simultaneously and set the priority levels when sending these campaigns (see Annex 3.03: Volumetrics). This applies to both Email and Mobile Messaging campaigns;

(d) the ability to pre-schedule campaigns for automatic delivery at specific dates and times, up-to one month in advance. The Authority must have the ability to make any changes to plans at short notice;

(e) the ability to schedule and issue messages 24/7/365, and also have the capability as and when required to restrict deployment and delivery within specified timeframes;

(f) the capacity to schedule campaigns with the option of batching and staggering issue times over specified timelines;

(g) the functionality to pause/stop/resume sending from specific and all campaigns, to respond in real-time to operational demands;

(h) the ability to create and inject courtesy copies into any given distribution lists prior to a campaign going live;

(i) the ability to create and use dynamic customer contact distribution lists, from multiple data sources;

(j) acknowledgment email for both Email and Mobile Messaging upon deployment start and completion of campaign or event (to scheduler);

(k) the facility to allow configuration of strategies, campaigns and customer journeys without the need for hands-on technical support;

(l) the ability to upload entire campaign datasets en masse;

(m) the ability to manually manage, and/or apply business rules to, any unsent Emails and Mobile Messages;

(n) the ability to cross-check any suppressions lists before sending any communications and the ability for the Authority to override, where applicable (see Paragraph 5.10, Suppression lists).

5.7 MARKETING CAMPAIGN EMAIL SPECIFIC REQUIREMENTS

5.7.1 The Supplier must provide the functionality with the ability listed below required by the Authority:

a) to set send criteria to manage the frequency of customer contact. These send criteria are to include logic such as:

(i) if, and, or statements;

(ii) send to amount; and

(iii) send parameters e.g., "if this then that" exclusions.

b) for any undelivered communications to be re-attempted if successful delivery is not made upon the first attempt;

c) to create, schedule and send a series of email communications or customer journeys to a specific group over specified timeframes;

d) to send from multiple domains, with a no-reply functionality, where applicable.

5.8 MOBILE MESSAGING SPECIFIC REQUIREMENTS

5.8.1 The Supplier must provide functionality with the ability for any undelivered Mobile Messaging communications to be re-attempted, for a minimum of 72 hours, if successful delivery is not made upon the first attempt.

5.8.2 The Supplier must provide the functionality where specified to restrict mobile messages to be sent to UK mobile numbers only (07XX, +447XX) and extract any landline, international, premium, invalid or duplicate numbers and supply details of any suppressed numbers.

5.9 DATASTORE

Datastore requirements

5.9.1 The Supplier shall establish and maintain a datastore which ensures the marketing distribution lists are dynamically created from the most current information available regardless of original source.

5.9.2 The datastore must be capable of:

(a) merging customer topics of interest from both internal (information from the HODs and external sources (the Customer Preference Portal-Paragraph 5.11);

(b) allowing users to update subscription status of all external topics and specified internal topics via the Customer Preference Portal with “one-click” operation.

5.9.3 When customer lists are uploaded from internal sources specifying a particular topic of interest the upload process must:

(a) check if the customer already has an active record (either generated through external sign-up to the Customer Preference Portal or from a previous import);

(b) create a new customer record if one does not exist;

(c) enable the Authority to specify if the topic to be added to the customer record should become visible to the customer when accessing the Customer Preference Portal.

5.9.4 The Supplier datastore must accommodate a mechanism for customers to subscribe, unsubscribe and resubscribe to advertised topics without the need for either the Authority’s internal teams or Supplier intervention including;

(a) a customer who has unsubscribed from a particular topic should have this flagged within the customer record so that it is not overwritten when an internal upload is performed;

(b) a customer who decides to unsubscribe from all topics should have this flagged within the customer record so that it is not overwritten when an internal upload is performed;

(c) the customer must be able to resubscribe to any visible topic published via the Customer Preference Portal at any time.

5.9.5 The new datastore must allow the Authority to develop and grow its digital marketing offering, with future ambitions of incorporating the contact logging of communications invoked via Transactional Emails through the use of exposed APIs. It is envisaged that this will be through a non-relational datastore.

5.9.6 The Supplier shall engage with both the incumbent supplier and the various Authority internal teams to extract, cleanse and de-duplicate the data held within the current datastore prior to creating new customer records (most likely identified by email address). (**REDACTED**).

5.9.7 The Supplier must migrate customer records from the incumbent suppliers datastore, cleanse, de-duplicate and reformat this data to create individual customer records which specify the topics to a given customer and the visibility status (within the Customer Preference Portal) of internally subscribed topics generated through HODs export/import activities as detailed in these use cases.

5.9.8 The datastore must be capable of recording all email attempts within the same customer record however this is in addition to, not in replacement of the requirements detailed in respect of campaign reporting (see Paragraph 5.13).

5.9.9 The supplier must ensure a two-way secure data transfer mechanism, in line with the Authority's security policies (see Paragraph 5.23). This will include data transfer via User Interface, API and any other data transfer mechanisms between the Authority and the Supplier.

5.9.10 The datastore must be customer centric and scalable as per the Authority's requirements, which contains all customer contact information (the customer record) including but not limited to variables such as:

(a) subscribed topics;

(b) unsubscribed topics;

(c) and in respect of future evolution values such as customer name and language preference which can be added immediately by the Authority as required (hence the recommendation to utilise a non-relational/NoSQL database format where .xml files carry fields as tags which can be added as required).

5.9.11 The Customer Preference Portal must link into the datastore. The Authority must have the ability to update items such as visibility of topics for customers to create dynamic campaign distribution lists.

5.9.12 The datastore must:

(a) be accessible, configurable and manageable by both Parties;

(b) have the ability to upload and manage mass data sets incorporated to new or existing customer records within the datastore;

(c) include the ability to log all campaign communications and link back to the template used so that a fully rendered replica of the original communication can be viewed by appropriately authorised representatives of the Authority.

5.9.13 The Authority must have the ability to create, amend and remove customer data from distribution lists which will be derived from the Supplier hosted portal and the Authority's sourced data. All Email and Mobile Messaging transactional data is securely deleted from the Supplier platform at the end of the retention period, where in certain circumstances, this can be stipulated otherwise by the Authority. Prior to the deletion or encryption of any data, the Authority must be notified and in agreement.

5.9.14 Any distribution lists that are not currently in use to be deleted. This must be approved by the Authority prior to any deletion requests.

5.10 SUPPRESSION LISTS

5.10.1 The Supplier shall provide a solution which gives the Authority the following requirements:

(a) the ability to migrate all current suppression lists from the incumbent supplier;

(b) the ability to create, maintain and archive multiple Supplier-held suppression lists which can be automated and manually added to or overridden. These must be held by the Supplier, however, needs to be exportable by the Authority, and maintained for the lifetime of the Contract. Suppression lists for Marketing Campaign activities will be managed by topic of interest as well as a global suppression list to include details of Hard-Bounce delivery receipts.

5.11 CUSTOMER PREFERENCE PORTAL

5.11.1 The Authority requires a Supplier-hosted service portal website to capture and manage customer communication preferences.

5.11.2 The Supplier must provide the ability to authenticate customers via Government Gateway, however this may not be immediately implemented.

5.11.3 The Authority must have the ability to control customer visibility of all external/internal and temporary topic distribution lists that they are subscribed to via the utilisation of the Supplier-created and administered datastore (see Paragraph 5.9).

5.11.4 The Portal must:

(a) enable customers to subscribe to, unsubscribe from and resubscribe to external (publicly facing) topics and where internal topics are marked "visible" these topics will similarly be available for unsubscription activities;

(b) allow the Authority to create, amend or delete existing subscription topics as required and to be able to control visibility of the topics within the Portal;

(c) provide the Authority must with the ability to manually add to and remove individual and grouped customers from suppression lists or unsubscribe lists.

5.11.5 The Supplier must provide a datastore for such preferences (see Paragraph 5.9).

5.11.6 The Supplier must provide the ability to issue confirmation emails, for example upon sign-up, unsubscription and resubscription.

5.11.7 The Supplier must provide the ability to understand customer engagement (one such example being an exit survey on unsubscription) and obtain the relevant MI.

5.11.8 The Portal must adhere to GOV.UK design standards and be fully compliant with WCAG 2.1AA Accessibility Standards, achieved through an accessibility audit conducted by the Authority, ahead of go live (see Paragraph 2.5.1).

5.11.9 The Supplier must publish a WCAG 2.1AA Accessibility Standards compliance through an Accessibility Statement on the Portal.

5.11.10 The hosted Portal must re-direct from the Authority's sub-domain and a valid SSL certificate shall be provided by the Authority.

5.11.11 There must be a published privacy notice.

5.11.12 The Supplier shall be responsible for creating and publishing a cookie policy.

5.11.13 The Authority requires access and control of the detailed analytics of the Portal usage.

5.12 TRANSACTIONAL EMAIL REQUIREMENTS

5.12.1 The Authority operates customer email communications based upon transactional data through HMRC digital (see Paragraph 5.15). The vast majority of these Transactional Emails are notifications that a customer has a new message within their secure inbox and advises them to log on through Government Gateway to view the new message.

5.12.2 The Supplier shall respond to significant seasonal variation between volumetrics of this service dependent upon key business events, such as Self Assessment peak in January. (see Annex 3.03: Volumetrics).

5.12.3 Invocation of a Transactional Email is performed via reception of a trigger to initiate customer contact through one of the HODs operated and results in an API post request to send a specific email template, stored internally by the Authority, and append a specified set of metadata headers.

5.12.4 **REDACTED**:

5.12.5 The Supplier shall provide an API endpoint to receive RESTful POST requests to send emails transactionally to customers with the following detail (not exhaustive but current) incorporated into the message headers:

a) customer Email Address;

b) template Used;

c) category/Source of Origin;

d) user Variable Tags - Currently three (3) max however this should be able to grow as required without change to the API request format or onward processing;

e) TLS v1.2 set optimistically.

5.12.6 Transactional send throughput must be a minimum of 160 transactions per second (“TPS”).

5.12.7 The Supplier shall operate a series of suppression lists which are defined by the utilised sub-domains used as “send-from” domains, currently Transactional Emails all existing as sub-domains and these will be expanded over time however the ability to add new domains as required should be able to be completed by the Authority and its appropriately authorised representatives.

5.12.8 The Supplier shall assist the Authority in migrating existing suppression lists from the incumbent supplier to their solution.

5.12.9 The Supplier shall ensure the live service will be migrated to their proposed solution without risk of domain reputational damage.

5.12.10 The Supplier shall provide a User Interface for the Authority's appropriately authorised representatives to administer the solution and generate utilisation reports. The Supplier shall ensure "out of the box" reporting is available with the ability to create bespoke reports.

5.12.11 The Supplier shall use outbound webhooks as illustrated in the target end-state solution diagram above to provide delivery receipts to the Authority's designated API end-points. The throughput TPS for sending of DR notifications should be a minimum of 120 TPS, however prior to this Contract, the receiving infrastructure for Delivery Receipts within HMRC's Digital MDTP environment was capped at 100 TPS therefore a queueing mechanism (such as MQ) shall be incorporated by the supplier to allow throttling and queueing of DRs above 100 TPS.

5.12.12 The solution must incorporate Single Sign on ("SSO") from multiple sources (see Paragraph 5.15).

5.12.13 The solution must incorporate 'bring your own key' ("BYOK") authentication for API request exchange.

5.12.14 The Supplier shall permit the transmission and reception of tracking pixels within the outbound emails sent to customers.

5.12.15 The Supplier shall ensure that all processing, storage and transmission (in so far as the external endpoint of the Supplier solution) is based within the UK.

5.12.16 The Supplier shall ensure that all support personnel are located within the UK and hold the appropriate security vetting for the categories of data (e.g., PII, HCI, Secret and Top Secret) that they may be exposed to or have access of (see Paragraph 2.2).

5.12.17 The solution must adhere to the Authority's security standards for data storage (encryption at rest) and encryption in transit.

5.12.18 Implementation of the solution must be planned to minimise impact to any live service operations – notably this would suggest that cut-over activities are performed outside of core business hours and likely over weekends to allow for the greatest implementation window:

(a) implementation activities must be approved and abide by conditions and constraints advised by the Authority's Change Approval Board ("CAB");

(b) implementation activities must incorporate robust and actionable roll-back planning in the event of unforeseen difficulties or failure within the submitted implementation plans;

(c) completion of implementation activities will be decided by the Authority upon completion of Post-Implementation Verification Testing ("PIV") in consideration of results from a recent base-line test conducted within one (1) week of the implementation activity commencing.

5.13 MANAGEMENT INFORMATION (MI) AND REPORTING

5.13.1 Detailed analytics, transactional and delivery MI for all campaigns must be provided to the Authority for all services and products, including those provided by third-party Suppliers.

5.13.2 Where services are provided by a third party or via a Sub-contractor relationship, the Authority requires the same level of MI.

5.13.3 A live dynamic dashboard is required that shows the real time information and historical reporting for all campaign data for email and mobile messaging.

5.13.4 The Authority requires the ability to run transactional reports that shows the real time and historical reporting for all campaigns/deployments for email and mobile messaging (e.g., open clicks).

5.13.5 The Supplier shall provide reports in the exportable format which enables the Authority to edit and manage as required such as CSV, TXT, or Excel. The contents of the reports should be agreed upon by both Parties. Examples of the types of report we currently collate (see Annex 3.01: Reports).

5.13.6 The ability for the Authority to configure and customise reports to contain the information we need, in real time as well as on a pre-scheduled basis.

5.13.7 The ability to restrict reporting based on user accesses/business areas.

5.13.8 The dashboard requires to have fully customisable reporting parameters of time periods.

5.13.9 The dashboard/reports required will consist of, but are not limited to:

(a) detailed analytics around the portal usage e.g., accesses, dropout rates etc;

(b) the ability to monitor and track campaign TPS;

(c) the ability to report on the delivery outcome for each message, at a holistic and transactional level such as suppressed, delivered, hard bounced, soft bounced, failed etc;

(d) live website traffic analytics for the Customer Preference Portal;

(e) where campaigns have been phased/batched there must be an option for reports on each phase or batch to be combined and displayed as a single report to avoid manual intervention;

(f) searchable individual customer record across all relevant customer data sources to ensure quality of communications journeys with full cross referencing and audit;

(g) detailed customer behaviours analytics via use of a tracking pixels and link redirect tracking, within emails, which can be broken down by email (campaign) or individual customer;

(h) the ability to differentiate between mobile message volumes and message parts e.g., 1 message over 3 message parts;

(i) there must be the ability to adapt reporting capabilities for future Mobile Messaging options.

5.14 GENERAL SERVICE REQUIREMENTS

Connectivity and Integration

5.14.6 The Supplier shall provide and configure any hardware and/or software needed to integrate and be fully compatible with the Authority's systems.

5.14.7 The Supplier shall be required to support VPN connectivity for integration.

5.14.8 The exchange of digitised content between Parties via a secure link in the prescribed format using RESTful APIs with JSON payloads.

5.14.9 The Supplier shall detail the connectivity requirements of the solution, the protocols and the ports utilised (where known) and any unchangeable port assignments clearly specified.

5.14.10 Open API integration with 3rd party applications and robotic processing, where required.

5.14.11 **REDACTED**.

5.15 SYSTEM ACCESS AND ADMINISTRATION5

5.15.1 The system must be intuitive and easily accessible through integration with the Authority's single sign-on via Azure active directory and HMRC Digital's domain controllers. There are 2 user groups – HMRC core and HMRC Digital. These reside on separate Active Directory forests and therefore there is a need to federate with multiple IDPs.

5.15.2 The Authority requires the ability to create, manage roles and access, segment groups/teams, segment individual user access based on created user roles within the User Interface, for example, but not limited to, campaign user, super user and administrator.

5.15.3 User admin details must show individual and their allocated roles and accesses. The product must support externalisation of role allocation and a method of provisioning user data.

5.15.4 The user logs must be fully auditable, and the Authority must be able to access these.

5.15.5 A minimum of 50 concurrent platform users with the ability for users to simultaneously schedule campaigns, with no limit on the number of the Authority's users subscribed to the platform.

5.15.6 The platform will time out users that have been inactive for 30 minutes.

5.16 SUPPORT

5.16.1 The Supplier must provide 24/7/365 support via telephone or specific contact points (email)/escalation routes to resolve issues.

5.16.2 The Supplier shall ensure that all processing, storage and transmission (in so far as the external endpoint of the Supplier solution) and access to the Authority's data is based within the UK. Supplier access to the Authority's unencrypted data must be based within the UK and have the appropriate security vetting (see Paragraph 2.1).

5.17 **INCIDENT MANAGEMENT**

5.17.1 Incident management should cover anything which causes an interruption or a reduction in the quality of the service included but is not limited to security, IT and operational incidents.

5.17.2 The Supplier shall provide support for issue resolution, regardless of whether the root cause lays with the Supplier, Authority, or both.

5.17.3 The Authority's priority levels are outlined below:

(a) the response time is the target time from the time an incident report is logged with the Supplier to the time an initial response is sent back to the Authority;

(b) the resolution time is the time that the Supplier commits to restore the service to a level acceptable to the Authority.

5.17.4 The Authority requires the ability to manage the status and priority of support tickets.

Priority Level	**Application issues description**	**Response time**	**Resolution times**
Priority 1	Service unavailable or 50%+ users unable to access the service, failure of communications outputs to the public, or an incorrect output likely to mislead the public.	15 Minutes	4 hours
Priority 2	Partial service outage or 10% to 50% of users unable to access the service, or business critical function unavailable or working incorrectly.	30 minutes	8 hours
Priority 3	Partial service outage or less than 10% of users unable to access the service, or non-business critical function unavailable or working incorrectly.	1 hour	24 hours
Priority 4	A single user unable to access the service, or issue with a particular function which disrupts or prevents normal processing.	24 hours	3 days (72 hours)
Priority 5	Issue with a particular function but normal processing can continue.	48 hours	5 days (120 hours)

5.18 UPGRADES

5.18.1 The Supplier shall ensure any routine maintenance takes place outside of standard operating hours (06:00 – 21:00 Monday – Friday and 06:00 – 1700 on Saturday) and must be non-disruptive.

5.18.2 Any software updates must be planned in advance, release cadence to be provided minimum six (6) months in advance. All planned maintenance must adhere to the Authority's change management policies (CAB approval) and be submitted with appropriate

forward notice period dependent upon the impact of any service outages along with details of an actionable regression plan.

5.18.3 In the event of an unsuccessful update, consultation shall be within one (1) hour and agree remediation activities to restore service.

5.19 CHANGE REQUESTS

5.19.1 All change requests should be managed in line with the procedures set out in Schedule 8.3 (*Change Control*).

5.19.2 There are 3 types of change requests that may occur:

(a) contract change requests (see Schedule 8.3 (*Change Control Procedure*));

(b) change requests; and

(c) statement of work will be used on projects.

5.20 TRAINING

5.20.1 The Supplier shall provide:

(a) a comprehensive training package tailored to each service (campaign and Transactional Email, Mobile Messaging, Customer Preference Portal, administration etc) during onboarding. This includes, but is not limited to, tutorials, opportunity to work through examples to consolidate learning, supporting notes/guidance. Additional training and support mechanisms to consolidate learning, bridge knowledge gaps and ensure users can use the Service effectively, is also required. The Authority requires the ability to utilise the training material internally as required;

(b) training through a combination of face-to-face and virtual sessions;

(c) additional support such as role-defined access training, before, during and after go-live to ensure successful implementation;

(d) a fixed timeline of training to allow teams to understand the flow of steps necessary to complete before go-live date;

(e) practical walkthroughs for each service. The teams must have the ability to explore the systems in a test environment before go-live;

(f) a commitment to provide advance notice for upskilling the Authority users following changes relating to system upgrades, if necessary.

5.20.2 The Authority has the right to sign off when the users are sufficiently trained.

5.20.3 The Supplier to allocate point of contact(s) during go-live that will support teams learning within each service.

5.20.4 The Supplier must provide the opportunity for the Authority to have access to regular check-ups with technical experts for live or ongoing issues and training needs, i.e., drop-in sessions.

5.20.5 The Supplier must provide self-serve online platform guidance/knowledge base, which is easily searchable including an A-Z glossary of terminology used within the content relating to each service.

5.21 **VOLUMES**

5.21.1 The estimated annual volumes are as follows:

(a) **REDACTED**.

5.21.2 Volumes are subject to annual fluctuations and the volume profiles are included in (**REDACTED**). These volumes are provided for the purposes of supporting supplier bids and are not guaranteed. The Authority is exploring the use of The Authority is exploring the use of other mobile messaging communications (such as RCS & AMB) and therefore there are no volumes for these capabilities prior to entry into this Contract.

5.21.3 The Service must be scalable with the ability to handle burst capacity and fluctuations in volume without requiring impactful infrastructure changes or additional costs.

5.21.4 The Authority requires the ability to configure the TPS for each campaign.

5.21.5 The Authority require a minimum of:

(a) 150 TPS for SMS;

(b) 160 TPS for Transactional Emails;

(c) 480 TPS for Marketing Campaign Emails;

With the ability to segment TPS;

5.22 **Campaign Emails and Mobile Messaging specific requirements**

Testing - Email and Mobile Messaging

5.22.1 **Transactional Emails**

5.22.2 The Supplier shall form a critical part in the end-to-end automated process of delivering data driven email notifications to the Authority's customers. Integration and performance volume testing ("PVT") will be triggered and performed by the Authority to ensure the Supplier's services are fully integrated with the Authority's IT estate and the Supplier's services can meet the volume demand. The Supplier shall provide additional instances of their service and connect to the Authority's test and preproduction environments. Log files from the Supplier's system are required by the Authority to monitor the testing and to record results.

5.22.3 **Marketing Campaigns**

5.22.4 User acceptance testing of Marketing Campaign service will in the main be manual and carried out by the intended users of the service. Technical resources within the Authority will support the testing of the design and composition element to ensure the service generates output to the specified requirements. The customer facing Preference Portal will be tested by the Authority's accessibility team to ensure the latest accessibility and government design standards are met. The Supplier shall carry out internal testing of all their services before handing to the Authority for further testing.

5.23 **SECURITY**

5.23.1 The Supplier shall have a system infrastructure consisting of a minimum of two locations hosted in the UK, which must be accredited with UKAS ISO-27001. The Supplier must ensure that each location is accessible by a discrete internet addressable domain.

5.23.2 The Supplier Solution must:

(a) ensure compliance with relevant essential security requirements throughout the term of the contract;

(b) support the open telemetry specifications to enable monitoring;

(c) ensure that data is logically separated between customers and be uniquely encrypted per customer;

(d) design robust service resilience into the Service both technically and within support models in line with 'The UK Government Resilience Framework' and present the support model service level agreements to the Authority;

(e) provide evidence via audit reports that ISO27001 security standards or NIST 800 are adhered to, and the in-operation evidence of organisational security compliance is ISO or SOC2;

(f) check approved open testers on an annual basis or such time as both Parties agree;

(g) have a security patch management system and apply patches as soon as possible but not later than N-1;

(h) ensure there are security controls in place to monitor, detect, prevent anomalous or unauthorised activity with the premises/environment;

(i) ensure all user actions and automated system actions are logged to ensure security is not compromised;

(j) ensure DMARC/DKIM/SPF are applied as additional security controls;

(k) ensure the Authority will be able to bring its own encryption keys;

(l) ensure that security logs are searchable, actionable and exportable to external systems by appropriately authorised resources;

(m) have the ability to protect and report against phishing and smishing;

(n) ensure that Information Lifecycle Management policies are implementable for all data retained in the solution;

(o) ensure that data is retained for only as long as agreed with the Authority. In specific cases, the Authority may ask the Supplier to retain data for longer, e.g., to be used for evidential output purposes;

(p) ensure that data is encrypted at rest using unbroken algorithms. At a minimum, this will be at a minimum AES256 or equivalent;

(q) ensure that where required, data must be encrypted in transit using unbroken algorithms. At a minimum, this will be at least TLS 1.2 (Transport Layer Security) for web traffic.

6 Part D -Transition Requirements

6.1 TRANSITION SERVICES

6.1.1 The Transition period is targeted as 12 months and must be completed no later than 18 months from commencement of discovery. The schedule of dates for services to transition shall be agreed during transition planning however they may be subject to change

depending on business need. Where applicable any new Supplier shall work cooperatively and in partnership with the Authority and incumbent Suppliers, to understand the full scope of Services and ensure a mutually beneficial handover of those Services. During this transition, the Authority expects that there will be a period of hybrid working with the incumbent and new Supplier. This will be agreed during the Discovery Period.

6.1.2 The Supplier must provide to the Authority an organisational structure of key personnel, their accountabilities and security clearance status. The Authority will issue the same information to the Supplier.

6.1.3 Transition of the Services may take the form of hybrid working where certain activities are delivered under the new Contract and some remaining with the incumbent suppliers. Timelines will be agreed during the transition planning period.

6.1.4 If there is to be a period of hybrid working, the Supplier shall ensure optimal communication with the incumbent Supplier and the Authority's chosen service providers so as to ensure no disruption to service. Approval of hybrid working must be approved by the Authority.

6.1.5 Email & Mobile Messaging must take place during specific transition windows as indicated below. These windows may be subject to change due to operational demand.

(a) Marketing Campaign: September – October;

(b) Transactional Email: September – November.

6.1.6 The Supplier must ensure Transition of Services without adverse impact to the business.

6.1.7 Implementation of the solution should be planned to minimise impact to any live service operations. Cut-over activities must be performed outside of core business hours and/or over weekends to allow for the greatest implementation window.

6.1.8 The Authority and Supplier shall agree on the transition of the individual services for each service line e.g., Email & Mobile Messaging (Marketing Campaign Email, Transactional Email, campaign SMS, and Mobile Messaging).

6.1.9 In respect of Email & Mobile Messaging, the Supplier shall migrate live service to their proposed solution without risk of domain reputational damage.

6.2 **DISCOVERY PERIOD**

6.2.1 The Supplier shall work with any incumbent suppliers and the Authority throughout the Discovery Period to gather information about the requirements and form precise boundaries. The goal of the Discovery Period is to plan a seamless transition for each of the

Services without interruption to current service levels and service delivery, and to reduce and mitigate all risks connected to the transition phase.

6.2.2 As a minimum the Supplier is required to:

(a) finalise and maintain a register of Risks, Assumptions, Issues and Dependencies (RAID or similar such as CRAIDL or MART);

(b) finalise and maintain an activity plan inclusive of a RACI Matrix and transitional milestones;

(c) outline areas to target knowledge share to include, but not limited to:
(i) service Overviews;
(ii) incident Management;
(iii) change Management;
(iv) scheduled events;
(v) service levels;
(vi) performance Reviews and MI Reports;
(vii) security clearance;
(viii) the Authority's postal providers.

(d) Output Specific Items:
(i) MyBUY catalogue;
(ii) agree other aspects of the rate card with the Authority, including the c.500 Forms Fulfilment products; and
(iii) to agree paper and manilla envelope price review indices.

6.3 **TRANSITION PLAN**

6.3.1 The Supplier shall assess the scope of the Services and prepare an outline transition plan, as per Schedule 6.1 (*Transition*) to be presented to the Authority. The Authority will then work in collaboration with the Supplier to agree and sign-off the detailed transition plan.

6.3.2 The outline transition plan will detail how the key priority deliverables will be achieved, including but not limited to:

(a) solution design, build, development and integration activities, including timelines;

(b) the timely delivery and testing of all Services requirements;

(c) the transfer of records/products/stock/consumables from the Authority and incumbent Supplier where applicable;

(d) security clearance for Supplier personnel (working in conjunction with the Authority to understand lead in times and ensure that relevant Supplier personnel are identified to the Authority at the earliest opportunity to commence the process);

(e) activities to fulfil the requirements of the Authority's postal providers, (for example to include site assessments to understand entry points, vehicle access equipment required etc);

(f) timescales shall be agreed with the Authority and aligned with the Authority's internal approval processes e.g., Technical Design Authority.

6.3.3 The Supplier shall appoint a Contract or Transition Manager(s) who shall be responsible for the management of the transition period and provide written notification of such appointment to the Authority within two (2) weeks of the Effective Date.

6.3.4 The Supplier shall maintain relevant activity and management plans e.g., RAID or similar in accordance with Paragraph 6.8 of Schedule 6.1 (*Transition*).

6.3.5 The Authority acknowledges that, following the Discovery Period, updates to the Transition plan may be needed. Any material amendments to the Transition Plan shall be subject to the Change Control Procedure set out in Schedule 8.3 (*Change Control*). Any other amendments are subject to the process set out in Paragraph 4 of Schedule 6.1 (*Transition*).

6.4 **OUTPUT SERVICES SPECIFIC TRANSITION REQUIREMENTS:**

Postal provision during the transition period

6.4.1 The Supplier shall facilitate site assessments of collection points by the Authority's chosen mail service providers, as required. This includes assessment of entry points to site(s), vehicle access, equipment to be used, personnel involved with the despatch of mail, requirements for consumables and storage of consumables if required. This also includes an assessment of the volumes forecast, mix of products (for example, 1st class, 2nd class etc).

6.4.2 The Supplier shall work with the Authority's chosen mail service providers to ensure any appropriate training needed by the Supplier's personnel is requested and provided in advance.

6.5 EMAIL & MOBILE MESSAGING SERVICES SPECIFIC TRANSITION REQUIREMENTS

6.5.1 The Supplier must work with the Authority to:

(a) port the Authority's existing short code on a date agreed with the Authority, during Discovery Period;

(b) transfer any Mobile Messaging registrations, such as Rich Communication Services ("RCS"), Apple Messages for Business ("AMB") etc;

(c) migrate, cleanse, de-duplicate and import the data held within the incumbent supplier's current datastore, prior to creating new customer records (see paragraph 5.9.7);

(d) migrate existing campaigns currently operating via API connections, which will include campaigns triggered through other services/third-party suppliers;

(e) migrate and/or recreate existing templates for email and SMS. The Authority will provide the content and digital assets.

6.6 TESTING (OUTPUT SERVICES SPECIFIC)

6.6.1 The full library of letters and forms will not require end to end or physical production testing with the Supplier. The transition test plan will focus on ensuring the Supplier's IT systems are properly integrated with the Authority's IT estate and the customer communications platform in particular. The test plan will also focus on covering key printed outputs and all production profiles.

6.7 TRANSACTIONAL PRINT

6.7.1 The Supplier shall receive files from the Authority's test and preproduction environments ensuring test outputs are printed but not posted. The Supplier can also expect control go live testing within the production environment where end to end testing in the test environments is not achievable. The Authority must approve the test files prior to transition.

6.7.2 **REDACTED**. The Supplier shall be responsible for ensuring final print outputs are processed correctly according to the Authority's Output Handling Instructions. The Supplier may be

required to provide digital copies of all products printed for the first time to check the print file contains the correct output.

6.8 DIGITAL BOUNCE BACKS

6.8.1 The end-to-end journey of sending digital communications to the Authority's customers involves sending the customers a printed output where the Authority has failed to make contact digitally. The Authority will perform end-to-end testing which will result in test print files being produced which the Supplier shall be required to print.

6.9 PAYABLE ORDERS AND PAYSLIPS

6.9.1 Payable Orders and Payslips will require additional testing and the Supplier shall be responsible for ensuring the outputs meets the Pay.UK and the Cheque and Credit Clearing Company standards. Outputs from Payable Orders & Payslips test files will require testing by external suppliers **REDACTED**. The Supplier shall securely courier these outputs which will be coordinated by the Authority's Corporate Finance Team. These suppliers may change during the life of the Contract and the Supplier shall work collaboratively to ensure the continuity of the payslip processing.

6.10 INTEGRATION WITH INBOUND SCANNING

6.10.1 All printed outputs that form part of the inbound scanning journey will require testing. The Authority will provide test files for the Supplier to print and fulfil and distribute for inbound scanning testing.

6.11 HMRC CENTRAL PRINT SERVICE (HCPS)

6.11.1 The Supplier shall support in the end-to-end testing of the Authority's Central Print Service. The Authority will sign off the test outputs in the same way as the Transactional Print outputs. The Supplier will support with conducting specific end-to-end integration testing to ensure MI data relating to HCPS print files is reported back to the Authority.

6.12 FORMS FULFILMENT

6.12.1 The Supplier shall provide finished physical outputs of test files provided by the Authority to ensure supplied PDF artwork are printed to satisfactory standards.

6.13 ORDERING PROCESS

6.13.1 End-to-end testing will be performed by the Authority to ensure the Supplier can receive the data via the Authority's Data Exchange Service. The Authority will conduct end to end

testing resulting in test requests being submitted where the Supplier shall process the request.

6.14 **TESTING (INPUT SERVICES SPECIFIC)**

6.14.1 The Supplier shall provide support to the Authority to conduct integration and system testing of the Authority's IT services that ingests digitised mail from the Inbound Supplier.

6.14.2 **Structured and Non-Structured Mail – letters and forms:**

(a) **For Non-structured** - the Supplier shall generate test mock cases and subsequently process for the Authority to test the downstream IT systems and that mail items land as expected in DMS.

(b) **For Structured** - the Authority will supply test forms to enable appropriate testing of data extraction and transfer to downstream IT systems. Specific integration testing will be conducted by the Authority to ensure the Supplier is able to transfer data via the specified interface and data formats.

(c) **Evidential Scanning -** the Authority will supply test cases to the Supplier and the Supplier shall carry out end- to-end testing of the processing of Evidential Scanning requests, ensuring the returned outputs are transferred back to the Authority's IT system in the mediums described in the requirements.

(d) **Back Scanning** - the Authority will supply test cases to the Supplier and the Supplier shall carry out end-to-end testing of processing Back Scanning requests, ensuring the returned outputs are transferred back to the Authority's IT system and land as expected in DMS.

(e) **Returned Letter Service Data Extraction** - the Authority will supply test cases to the Supplier and the Supplier shall carry out end to end testing of processing returned mail, ensuring the returned outputs are transferred back to the Authority's IT system and data extracted correctly.

(f) **Online Portal** - the Supplier must demonstrate the portal functionality as per the specification including an accessibility audit.

6.15 **Testing (Email & Mobile Messaging Services Specific)**

6.15.1 The Supplier shall test in the following way:

(a) test SSO and access to the User Interface ahead of Transition of Service;

(b) build, and internally test a Customer Preference Portal. The content and design must be approved by the Authority (see paragraph 5.11);

(c) this Portal must undergo an accessibility audit (conducted by the Authority) and be fully approved by the Authority prior to Transition of Service.

DEFINITIONS

In this Schedule, the following definitions shall apply:

"A/B Deployments"	means the running of two (or more) versions of the application code or application configuration at the same time for testing or experimentation purposes;
"Assured Forwarding / AF"	enables different AF levels to be assigned to prioritise traffic on a network;
"Application Programming Interface / API"	is a set of subroutine definitions, protocols, and tools relating to methods of communication between various components;
"Archive Scanning"	means the process of scanning papers stored in a paper archive, for storing in a digital archive;
"Azure AD"	means **Azure Active Directory**. It manages roles and permissions;
"Back Scanning"	means the process of scanning papers stored in a paper archive, or those that would otherwise be stored in that way, and

	storing as a closed mail item within The Authority's Digital Mail Service;
"Batch Header"	for Input Services, means a template placed at the front of documents by the Authority that provides Scanning instructions for the Supplier; for Output services, means a template placed at the front of printed output produced by the Supplier, outlining details of the output to the recipient;
"Batch Interface File"	for Evidential Scanning, means a zipped file created by the Supplier containing scanned evidential documents;
"Business As Usual" or "BAU"	means regular daily/monthly activity;
"Bespoke Mailing"	is a one-off printed mailing to a selected customer group;
"Box Splitting"	means the process whereby mail received by the Supplier or Sub-contractor from the Authority's network offices is split up according to the target Queue Structure and receipt date(s);
"Business Service Indicator / BSI"	means a portable non-geographic address supplied by Royal Mail Retail (part of Royal Mail Group Ltd), from which mail is delivered directly to the Authority's scanning provider;
"Caseflow"	is the Authority's generic electronic case-management IT system, designed to help manage the full lifecycle of Compliance checks. Scanning to this system should conform to BSI10008;

"Central Mail Unit"	is the Authority's central function responsible for the handling of all residual incoming and outgoing paper-based mail, and the internal distribution of mail (including exceptions);
"CESA"	means **Computerised Environment for Self-Assessment**, which is one of the Authority's Heads of Duty Systems;
"Cheque and Credit Clearing Company Standards"	means the standards as set out by Pay.UK in relation to the printing of Cheques and bank giro credits;
"Child Benefit"	means benefit under Part I of the Child Benefit Act 1975;
"Communications Electronics Security Group / CESG"	is part of National Cyber Security Centre which acts as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents;
"Classify / Classified / Classification"	means the process of identifying which workflow a mail item should be assigned to. Primarily, this will be based on a Keyword or phrase. The Authority has a Keyword Matrix for each workflow structure;
"Cloud Management Platform / CMP"	is an integrated product used for the management of public, private and hybrid cloud computing environments;
"Compliance"	is a functional and process related activity carried out by the Authority, to ensure that it collects the full and correct amount of money due from UK taxpayers, investigates offences against the tax system and the targeted financial support it provides, and

	takes action to identify and mitigate potential threats;
“Control List”	is an XML file used by the Scanned Document Import Service to keep a track of the files it has to import and their current status within the import process;
“CSV”	means **Comma Separated Values** file, which is a plain text file that contains a list of data;
"CT "	means **Corporation Tax**;
"Core Services"	means those services that are critical to the Authority;
"CF"	means **Corporate Finance** – A team within The Authority;
"Customer ID’s "	are unique identifiers that are attributable to a customer and/or employer that are found within post items and transferred to the Authority as part of the metadata for ingestion to the Authorities processing systems;
"Customer "	is a person or business that communicates with the Authority by paper;
"DES"	means **Data Exchange Service**;
"Despatch Note"	is a manifest providing the key details of a shipment;
"DM"	means **Debt Management** – A team within the Authority;
"Dots Per Inch / DPI"	is a currency for resolution of images;
"Digital Mail Service / DMS"	is the Authority’s workflow system;

"Digital Mail Room"	is a facility that automates incoming mail processes, by providing document scanning and capture technologies;
"Digital Service Organisation"	means the type of organisation the Authority intends to be when it moves away from paper outputs and towards being a digital organisation where the majority of its interactions are paperless;
"DKIM"	means DomainKeys Identified Mail, which is an email authentication method that uses a digital signature to let the receiver of an email know that the message was sent and authorised by the owner of a domain;
"DMARC"	means **Domain-based Message Authentication, Reporting & Conformance**;
"Down Stream Access"	is where a mail service provider collects and sorts business mail before using Royal Mail's delivery network for the final state of distribution;
"DR"	means **Disaster Recovery**;
"Duplex"	means both sides of a sheet of paper;
"Emp Payee Ref"	means **Employer Pay As You Earn Reference** number;
"ENVA"	is a unique reference given to each envelope by the Supplier. This must be in the format ENVA12345678 and be sequential from the last used ENVA reference and form part of the data transferred to the Authority;
"Expedited Forwarding / EF"	provides low loss, latency, and jitter in network;

"E2E (End to End) Traceability"	for Input Services means a record of the movement of mail items and relevant reference numbers/codes from the moment they are received by the supplier to the stage where they are sent to the Authority (digital and physical mail items) and all stages in between; for Output services, means a record of the journey of the outputs from receipt of the file to print by the Supplier until despatch to customers;
"Extended Physical Interface Definition Document / EPIDD"	is an interface control document, providing a description of the data exchange and technical detail;
"Evidential Scanning"	means conversion of paper records under British Standard BSI BIP 0008, to legally admissible electronic records that will be accepted as evidence in court;
"Exception Items (Pre-scan and Post-scan)"	an exception is a mail item that is either unscannable or an item that the Authority has identified as an exception to the Scanning process. A list of examples is provided within the MSOG. These will be updated by the Authority as required;
"Exchequer"	means the accounting process of central government and the government's current account;
"File Transfer Protocol / FTP"	is the standard network protocol used for the transfer of computer files between a client and server on a computer network;
"File Transfer Protocol Secure / FTPS"	is a secure file transfer protocol based on FTP;

“Fraudulent Activity Incident”	means the intent or act of misrepresentation or illegal activities undertaken by an individual or company to cause gain or loss e.g., setting up an illegitimate company for tax evasion purposes;
“FTPS VPN”	means **File Transfer Protocol Service Virtual Private Network**;
"Golden Hour "	means a period when resources and capability will be at maximum levels to meet service level agreements;
"Government Security Classifications / GSC"	mean the physical, personnel and information security controls required to provide a proportionate and robust level of protection for assets at each of the security classifications;
"Handprint Forms"	mean forms that are printed off and completed by hand;
“HCI”	means **Highly Confidential information**;
"Head of Duty System" or “HODs”	means the Authority's back end transactional processing systems and key digital data records of customers;
“Health and Safety at Work Legislation”	means legislation owned and enforced by the Health and Safety Executive and Local Authorities, including the *Health and Safety at Work etc Act 1974* and other primary legislation, as well as applicable regulations;
"Hyper Text Markup Language / HTML"	is the standard language that the Authority requires to be used, where specified;

"Hypertext Transfer Protocol / HTTP"	is the type of interface that the Authority requires to be used for secure communication;
"Infrastructure as a Service / IaaS"	are online services that provide high-level APIs used to de-reference various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc;
"Index / Indexing"	means the process of associating an attribute with a PDF image, so that the image can be searched for. Primarily, Indexing is to be based on Customer identifiers, for which the Authority will provide a matrix for specific mail items. Other attributes will need to be used in the event of Back Scanning, e.g., the Authority's Business, Assets and International team need to be able to search based on a subject;
"ICR"	means **Intelligent Character Recognition**;
"Information Lifecyle Management Policies"	is a comprehensive approach to managing an organisation's data/ associated metadata and the practice of applying certain policies to effective information management;
"Internet Protocol Security / IPSec"	is one of two common VPN protocols, or set of standards used to establish a VPN connection;
IT Change Request	means changes to either: integration infrastructure, data formats including print files, document composition, production capabilities, testing and or go live processes.

	It could also include a request to produce a Bespoke Mailing campaign;
"IT Service Management / ITSM"	refers to the entirety of activities performed to design, plan, deliver, operate and control information technology (IT) services;
“Joint Business Plan”	is an agreement between the Parties that defines their common objectives, financial goals, growth, and shared business initiatives for the benefit of all Parties;
“JPEG”	means **Joint Photographic Experts Group**, which is a standard image format for containing lossy and compressed image data;
“JSON”	means **JavaScript Object Notation**, which is a standard text-based format for representing structured data based on JavaScript object syntax;
“Key Business Event(s) (KBE)”	mean periods of key business activity during the year for the Authority and its customers, such as Self-Assessment peak or Tax Credits peak;
"Keyword"	means a word, or phrase (e.g., changed my bank details), or a Ref format (e.g., 123 C 4567891011), used to Classify a mail item;
"Keyword Matrix"	is a document providing the list of Keywords to be used for Classification of mail items into a given queue;
"Management Information / MI"	means information on operational performance;
“Marketing Campaign”	means one-to-many email or SMS communications providing help and support

	on various tax or benefit-related topics, and MP and Parliamentary communications;
"MSOG"	means **Mail Services Operating Guide**;
“MyBUY”	is an online workspace for procurement in the Authority which supports purchase ordering, receipting and invoicing;
“N-1”	a power system can be described as being N-1 secure when it is capable of maintaining normal operations in the event of a single contingency event, such as the unplanned loss of a transmission line, generator or transformer;
“NEP”	means **New Employer Pack**, which new employers receive when starting up and which provides them with their employer registration and Accounts Office reference numbers, information about paying HMRC electronically and a link to the PAYE payment advice on GOV.UK;
"NICEO RLS"	means Postal items returned to the Authority by Royal Mail as not at that address, specifically for the National Insurance and Employers office;
"NINO"	means **National Insurance Number**;
"No.10 Transparency Reporting"	is reporting that the Authority is required to make, to inform information that HM Government is publishing under its openness and transparency agenda;
"Non-structured” or "Non-structured Mail"	means letters and forms received from the Authority’s customers;

"NPS"	means **National Insurance & PAYE Service**. This is one of the Authority's Heads of Duty Systems;
"Optical Character Recognition / OCR"	means the identification of printed characters using photoelectric devices and computer software;
"Oauth"	means **Open Authentication**. It is an open standard used for authentication;
"Order lines"	means the number of orders of forms placed. It does not mean the number of actual forms ordered, as each Order Line may contain multiple requests for forms;
"Output(s)"	mean(s) any outbound printed product(s) from the Authority to its customers;
"Outputs Planning & Governance Board"	is a monthly meeting involving key stakeholders and suppliers to review and obtain agreement to the despatch of outputs planned for two (2) months in advance;
"Output Handling Instructions"	means an instruction manual containing all HMRC print products, requirements such as inserts, perforations etc, service level agreements and despatch methods, required to deliver the print outputs;
"Payable Orders"	is a payment method in the form of a cheque;
"Pay.uk Standards"	Pay.UK is the recognised operator and standards body for the UK's retail interbank payment systems or equivalent or replacement standard if amended or changed during the course of the Contract;

“PDF/A”	is a variation of the PDF format that ensures a document can be reproduced exactly the same way, regardless of what software is used**;**
“PII”	means **Personal Identifiable Information**;
"PT"	means **Personal Tax**;
"Platform as a Service / PaaS"	is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application;
“Print Ready Files”	means A file that is precomposed and does not require further composition;
"Portable Document Format / PDF"	is the format in which the Authority requires scanned images;
"Public Sector Network / PSN"	is the UK government's high-performance network, which helps public sector organisations work together;
"Push To Queue"	means a queue that only exists in the Authority’s domain to ‘push’ mail into as required (no Supplier activity or interface);
"Queue Matrix"	is an Excel worksheet setting out all the queues within the Authority’s workflow;
"Queue Structure"	is a hierarchical workflow structure, where mail is received at the top level and then Classified into one or more queues positioned below it;
“Raw Data File”	means a file containing data only;

“Real Time Information (RTI)”	is an HMRC system for the provision of PAYE information by employers;
"Representational State Transfer / REST"	is the architectural style for distributed hypermedia systems;
"Return Letter Service / RLS"	is mail issued by the Authority, which is returned as the customer no longer resides at the address;
"Red Hat Enterprise Linux / RHEL"	is an operating system;
"SaaS"	means **Software as a Service** - a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted;
"SAML"	means **Security Assertion Markup Language**, which is an open standard used for authentication;
"SIBP"	means **Security and Information Business Partner**;
"SCA"	means **Single Customer Account**;
"SCR"	means **Special Customer Records**;
“SCIDs”	means Supply Chain Identifiers: They enable customers, suppliers and Royal Mail Wholesale to be able to track the mail process and identify each separate part within the production and despatch of mail items. They also allow for identification of who is paying the invoices for this particular stream of mail;
"SDES"	means **Secure Data Exchange Service**;
“Seeding”	means where identifiers are included by the Supplier in the Authority’s mail so that the

	number of days from handover to Royal Mail to receipt can be tracked. This allows the Authority and Royal Mail to measure Royal Mail's quality of service specifically for the Authority's mail;
"Self Assessment"	is a system whereby taxpayers have the duty to give notice to the Authority that they are chargeable to tax, providing information to allow calculation of the amount of tax due;
"Service"	means any and all of the services to be provided by the Supplier under the Agreement, including those set out in this Schedule;
"Single Customer Accounts"	is an online account for HMRC customers to access their business and personal tax returns in one place;
"Single Sign on (SSO)"	is a session and user authentication service permitting a user to supply a single set of login credentials to access multiple applications with agreed permissions and access limits set centrally;
"SLA"	means service level agreement;
"Statutory Notice(s)"	means a statutory notice issued by HMRC in relation to the non-payment or late payment of tax, fines or other requests for money;
"SPF"	means **Sender Policy Framework**, which is **a standard email authentication method**. SPF helps protect one's domain against spoofing and helps prevent outgoing messages from being marked as spam by receiving servers. SPF specifies the mail servers that are allowed to send email for your domain;

“Statutory Payment(s)”	means a payment issued in accordance with an Act of Parliament;
"Structured” or “Structured Mail"	mean forms which the Authority have designed for data to be extracted and flowed through to the Authority’s back end transactional processing systems;
"Software und System-Entwicklung / SUSE"	is an operating system;
“Tax Administration”	How the government administers taxation;
"TRN"	means **Temporary Reference Number**;
“Transactional Email”	means an outbound customer email communication that is triggered by a transaction made on the Authority’s IT systems;
"Transactional Print"	means data driven customer correspondence which is triggered from an IT system and usually batched and printed in large volumes;
“Transition of Service”	means the transition of the Service from the incumbent supplier to a new Supplier;
"Tower Repository"	is the Authority’s digital storage repository for Structured Mail only (excluding Caseflow and NI ORU VAT 65);
“UI”	means **User Interface**;
“The UK Government Resilience Framework”	means the Cabinet Office’s policy paper entitled, ‘The UK Government Resilience Framework’, published 19 December 2022;
"UTR"	means **Unique Tax Reference**;

"Valuable Items"	mean original items such as passports, birth certificates, which need to be returned to the customer;
"Virtual Private Network / VPN"	a system which extends a private network across a public network;
"Virtual Routing and Forwarding / VRF"	a system which increases functionality by allowing network paths to be segmented without using multiple devices. VF also increases network security and can eliminate the need for encryption and authentication;
"VRN"	means **VAT Registration Number**;
“XML”	means **Extensible Markup Language**, which is a simple text-based format for representing structured information;
“24/7/365”	means 24 hours per day, seven days per week, 365 days per year.

HM Revenue & Customs

HMRC Tier 1 and 2 Model ICT Contract
Version 2.3 (December 2020)

SCHEDULE 2.2 | Performance Levels

OFFICIAL – SENSITIVE - COMMERCIAL

Schedule 2.2 | Performance Levels

1 DEFINITIONS

In this Schedule, the following definitions shall apply:

"Delivery Group"	means a business group within the Authority's operating model which is designated as such by the Authority for the purposes of this Agreement. The initial Delivery Groups for the purpose of this Agreement are Output Services, Input Services and Email and Mobile Messaging;
"KBE Notice" and "KBE End Notice"	has the meaning given at Paragraph 2.8 of Part A;
"Key Business Event"	means an event designated as such by the Authority from time to time;
"Operational Business Day"	means Monday to Saturday (inclusive);
"Performance Failure"	has the meaning given in Paragraph 1.7 of Part A;
"Performance Monitoring Report"	has the meaning given in Paragraph 7.0 of Part B;
"Performance Review Meeting"	the regular meetings between the Supplier and the Authority to manage and review the Supplier's performance under this Schedule, as further described in Paragraph 7.4 of Part B;
"Repeat KPI Failure"	has the meaning given in Paragraph 4.1 of Part A;
"Repeat SPI Failure"	has the meaning given in Paragraph 4.2 of Part A;
"Service Charge(s)"	the periodic payments made in accordance with Schedule 7.1 (Charges and Invoicing) and as referred to in Schedule 2.2 (Performance Levels), in respect of the supply of the Operational Services;
"Service Level Category"	means "Minimum", "Standard" and "Enhanced" categories for the Target Performance Level and the Severity Levels for each Performance Indicator (details of which are further set out in Part I of Annex 1);
"Severity Levels"	means, for each Performance Indicator, the bands or levels of performance falling below the Target Performance Level which determine the seriousness of the Supplier's failure, as determined in accordance with the tables in Annex 1 and which are further described in paragraph 1.7 of Part A.

ANNEX 1 | KEY PERFORMANCE INDICATORS AND SUBSIDIARY PERFORMANCE INDICATORS

PART I: KEY PERFORMANCE INDICATORS AND SUBSIDIARY PERFORMANCE INDICATORS TABLES

The Key Performance Indicators and Subsidiary Performance Indicators that shall apply to the Services and relevant Delivery Groups are set out below:

Table 1 - Key Performance Indicators

KEY PERFORMANCE MEASURES

(a) EMAIL & MOBILE MESSAGING KPIs

Performance Area	KPI 1 - Reliability
Delivery Group	Email and Mobile Messaging Services
Key Performance Indicator	**REDACTED**
Minor KPI Failure Service Points	**REDACTED**
Major KPI Failure Service Points	**REDACTED**
Description	Reliability Email and Mobile Messaging Services
Measurement Period	***Monthly***
Measurement Start Date (if not an Operational Service Date)	**Operational Service Date**
Method of calculation	**REDACTED**
Publishable Performance Information	NO

KPI Target Performance Levels and Severity Level Thresholds			
Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold	Critical Failure Performance Threshold
• **REDACTED**	• **REDACTED**	• **REDACTED**	**REDACTED**

Performance Area	KPI 2 - Service Availability
Delivery Group	Email and Mobile Messaging Services
Key Performance Indicator	**REDACTED**
Minor KPI Failure Service Points	**REDACTED**
Major KPI Failure Service Points	**REDACTED**
Description	Service Availability for Email and Mobile Messaging Services
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	**Operational Start date**
Method of calculation	**REDACTED**
Publishable Performance Information	NO

KPI Target Performance Levels and Severity Level Thresholds			
Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold	Critical Failure Performance Threshold
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**

(a) **OUTUT SERVICES KPIs**

Performance Area	KPI 3 - HCPS Printed Output
Delivery Group	Output Services
Key Performance Indicator	**REDACTED**
Minor KPI Failure Service Points	**REDACTED**
Major KPI Failure Service Points	**REDACTED**
Description	HCPS Printed Output
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	YES

KPI Target Performance Levels and Severity Level Thresholds

Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold	Critical Failure Performance Threshold
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**

Performance Area	KPI 4 - Category 1 Printed Outputs
Delivery Group	Output Services
Key Performance Indicator	**REDACTED**
Minor KPI Failure Service Points	**REDACTED**
Major KPI Failure Service Points	**REDACTED**
Description	Category 1 Printed Output
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	YES

KPI Target Performance Levels and Severity Level Thresholds			
Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold	Critical Failure Performance Threshold
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**

Performance Area	KPI 5 Category 2 Printed Outputs
Delivery Group	Output Services
Key Performance Indicator	**REDACTED**
Minor KPI Failure Service Points	**REDACTED**

Major KPI Failure Service Points	**REDACTED**
Description	Category 2 Printed Output - timeliness
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	YES

KPI Target Performance Levels and Severity Level Thresholds			
Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold	Critical Failure Performance Threshold
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**

Performance Area	KPI 6 - Forms Fulfilment
Delivery Group	Output Services
Key Performance Indicator	**REDACTED**
Minor KPI Failure Service Points	**REDACTED**
Major KPI Failure Service Points	**REDACTED**
Description	**REDACTED**
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date

Method of calculation	**REDACTED**
Publishable Performance Information	NO

KPI Target Performance Levels and Severity Level Thresholds		
Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold
REDACTED	**REDACTED**	**REDACTED**

Performance Area	KPI 7 - Security Breaches – Output Sevices
Delivery Group	Output Services
Key Performance Indicator	**REDACTED**
Minor KPI Failure Service Points	**REDACTED**
Major KPI Failure Service Points	**REDACTED**
Description	Security Breaches for Output Services
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

KPI Target Performance Levels and Severity Level Thresholds			
Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold	Critical Failure Performance Threshold
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**

Performance Area	KPI 8 - Reliability – Output Services
Delivery Group	Output Services
Key Performance Indicator	**REDACTED**
Minor KPI Failure Service Points	**REDACTED**
Major KPI Failure Service Points	**REDACTED**
Description	Reliability for Output Services
Measurement Period	***Monthly***
Measurement Start Date (if not an Operational Service Date)	**Operational Service Date**
Method of calculation	**REDACTED**
Publishable Performance Information	NO

KPI Target Performance Levels and Severity Level Thresholds			
Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold	Critical Failure Performance Threshold
• **REDACTED**	• **REDACTED**	• **REDACTED**	**REDACTED**

(b) **INPUT SERVICES KPIs**

Performance Area	KPI 9 - Non-structured scanning – timeliness and quality
Delivery Group	Input Services
Key Performance Indicator	**REDACTED**
Minor KPI Failure Service Points	**REDACTED**
Major KPI Failure Service Points	**REDACTED**
Description	Non-Structured Mail scanning – timeliness and quality, Input Services
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	YES

KPI Target Performance Levels and Severity Level Thresholds			
Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold	Critical Failure Performance Threshold

REDACTED	**REDACTED**	**REDACTED**	**REDACTED**

Performance Area	KPI 10 - Structured Mail Scanning
Delivery Group	Input Services
Key Performance Indicator	**REDACTED**
Minor KPI Failure Service Points	**REDACTED**
Major KPI Failure Service Points	**REDACTED**
Description	Structured Mail scanning – timeliness and quality, Input Services
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	YES

KPI Target Performance Levels and Severity Level Thresholds			
Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold	Critical Failure Performance Threshold
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**

Performance Area	KPI 11 - Evidential Scanning
Delivery Group	Input Services
Key Performance Indicator	• **REDACTED**
Minor KPI Failure Service Points	**REDACTED**
Major KPI Failure Service Points	**REDACTED**
Description	Evidential Scanning – timeliness and quality, Input Services
Measurement Period	As per the time for delivery agreed on a case by case basis
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	YES

KPI Target Performance Levels and Severity Level Thresholds			
Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold	Critical Failure Performance Threshold
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**

Performance Area	KPI 12 - Back Scanning
Delivery Group	Input Services
Key Performance Indicator	**REDACTED**
Minor KPI Failure Service Points	**REDACTED**
Major KPI Failure Service Points	**REDACTED**
Description	Back Scanning – timeliness, Inupt Services
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

KPI Target Performance Levels and Severity Level Thresholds			
Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold	Critical Failure Performance Threshold
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**

Performance Area	KPI 13 - Security Breaches
Delivery Group	Input Services
Key Performance Indicator	**REDACTED**
Minor KPI Failure Service Points	**REDACTED**

Major KPI Failure Service Points	**REDACTED**
Description	Security Breaches, Input Services
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

KPI Target Performance Levels and Severity Level Thresholds			
Target Performance Level	Minor Failure Performance Threshold	Major Failure Performance Threshold	Critical Failure Performance Threshold
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**

1.2 SUBSIDIARY PERFORMANCE INDICATOR

(a) EMAIL & MOBILE MESSAGING SPIs

Performance Area	SPI 1 - Incident Resolution
Delivery Group	Email and Mobile Messaging Services
Subsidiary Performance Indicator	**REDACTED**
Description	Incidents exceeding resolution time
Measurement Period	***Monthly***
Measurement Start Date (if not an Operational Service Date)	Operational Start Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

Performance Area	SPI 2 - Incident response time
Delivery Group	Email and Mobile Messaging Services
Subsidiary Performance Indicator	**REDACTED**
Description	Incident response time, Email and Mobile Messaging Services
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

Performance Area	SPI 3 – Forecast Accuracy - Campaigns
Delivery Group	Email and Mobile Messaging Services
Subsidiary Performance Indicator	**REDACTED**
Description	Forecast accuracy of communications deployment timeframes for Email and Mobile Messaging Services
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

Performance Area	SPI 4 – Scheduled Adherence - Campaigns
Delivery Group	Email and Mobile Messaging Services
Subsidiary Performance Indicator	**REDACTED**
Description	For Email and Mobile Messaging, communications are deployed as specified by the Authority.
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**N/A**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

(b) OUTPUT SERVICES SPIs

Performance Area	SPI 5 - Category 3 Printed Output - Bulk
Delivery Group	Output Services
Subsidiary Performance Indicator	**REDACTED**
Description	Category 3 Printed Output SPI
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

Performance Area	SPI 4 - Change and New Template Composition
Delivery Group	Output Services
Subsidiary Performance Indicator	**REDACTED**
Description	Change and New Template Composition for Output Services
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**N/A**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

Performance Area	SPI 5 - Incident Resolution – Output Services
Delivery Group	Output Services
Subsidiary Performance Indicator	• **REDACTED**
Description	Incidents exceeding resolution time for Output Services
Measurement Period	***Monthly***
Measurement Start Date (if not an Operational Service Date)	Operational Start Date
Method of calculation	**N/A**

Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

Performance Area	SPI 6 - Incident response time – Output Services
Delivery Group	Output Services
Subsidiary Performance Indicator	**REDACTED**
Description	Incident response time for Output Services
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

Performance Area	SPI 7 - Quality Assurance
Delivery Group	Output Services
Subsidiary Performance Indicator	**REDACTED**
Description	Quality Assurance for Output Services
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds

Target Performance Level
REDACTED

(c) INPUT SERVICES SPI

Performance Area	SPI 8 - Structured and Non-Structured Mail scanning
Delivery Group	Input Services
Subsidiary Performance Indicator	**REDACTED**
Description	Cheque Processing
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

Performance Area	SPI 9 - Structured & Non Structured Mail scanning
Delivery Group	Input Services
Subsidiary Performance Indicator	**REDACTED**
Description	Valuable Items – Timeliness
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

Performance Area	SPI 10 - Data Extraction and Scanning
Delivery Group	Input Services
Subsidiary Performance Indicator	**REDACTED**
Description	RLS
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

Performance Area	SPI 11 - Structured and Non-Structured Mail scanning
Delivery Group	Input Services
Subsidiary Performance Indicator	**REDACTED**
Description	Online Exceptions
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

Performance Area	SPI 12 - Structured and Non-Structured Mail scanning
Delivery Group	Input Services
Subsidiary Performance Indicator	**REDACTED**
Description	Physical pre-scan exceptions
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

Performance Area	SPI 13 - Structured and Non-Structured Mail scanning
Delivery Group	Input Services
Subsidiary Performance Indicator	**REDACTED**
Description	Re-scans and hard copy retrievals
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO

SPI Target Performance Levels and Severity Level Thresholds
Target Performance Level
REDACTED

Performance Area	SPI 4 - Structured and Non-Structured Mail scanning Quality Control
Delivery Group	Input Services
Subsidiary Performance Indicator	**REDACTED**
Description	Quality control
Measurement Period	Monthly
Measurement Start Date (if not an Operational Service Date)	Operational Service Date
Method of calculation	**REDACTED**
Publishable Performance Information	NO
SPI Target Performance Levels and Severity Level Thresholds	
Target Performance Level	
REDACTED	

1.3 SOCIAL VALUE KEY PERFORMANCE INDICATOR

Commitment Title	Commitment Description (What - will be delivered)	Actions (How will the Commitment be delivered)	Unit of Measurement	Target(s) (Why - Benefits and Outcomes)	Date/Timescale for Completion (When)	Reporting Period
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**

REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**

REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**

REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**

PART A | PERFORMANCE INDICATORS AND SERVICE CREDITS

1 PERFORMANCE INDICATORS

1.3 Annex 1 to this Schedule sets out the Performance Indicators which the Parties have agreed shall be used to measure the performance of the Services by the Supplier. The Target Performance Levels and Severity Levels which are applicable to this Agreement and for each Performance Indicator will depend upon and be determined by the Authority for the relevant Delivery Group.

1.4 Performance Indicators are broken down into Key Performance Indicators and Subsidiary Performance Indicators, the Supplier's performance of and against which the Parties have agreed will be measured.

1.5 NOT USED

1.6 The Supplier shall perform the Services so that they meet or exceed the applicable Target Performance Levels at all times.

1.7 Each Performance Indicator which relates to a Service shall apply and be measured from the relevant Operational Service Date of the relevant Service(s) to which that Performance Indicator relates (unless otherwise stated in Annex 1).

1.8 The Supplier shall monitor its performance of the Services against the Target Performance Level for each Performance Indicator and shall send the Authority a Performance Monitoring Report detailing the level of service and relevant level of performance actually achieved by the Supplier against each Performance Indicator in the relevant Measurement Period in accordance with the provisions of Part B of this Schedule.

1.9 The Target Performance Level is the minimum standard of performance which is required by the Authority. A **"Performance Failure"** will have occurred where the Supplier fails to provide any part of the Services in accordance with and so as to at least meet the relevant Target Performance Levels. Performance Failures are further divided into the following Severity Levels:

(a) a "Minor KPI Failure" or "Minor SPI Failure" will have occurred where the Supplier fails to provide any part of the Services to a level which meets or exceeds the Target Performance Level for the relevant Performance Indicator, but where performance meets or exceeds the relevant Major Failure Performance Threshold;

(b) a "Major KPI Failure" or "Major SPI Failure" will have occurred where the Supplier fails to provide any part of the Services to a level which meets or exceeds the Major Failure Performance Threshold for the relevant Performance Indicator, but, in the case of a KPI where performance meets or exceeds the relevant Critical Failure Performance Threshold (as appropriate) (if one exists)

(c) a "Critical KPI Failure" will have occurred where the Supplier fails to provide any part of the Services to a level which meets or exceeds the Critical Failure Performance Threshold for the relevant Performance Indicator. It is acknowledged and agreed by the Supplier that the Critical Failure Performance Threshold level has been set for the most critical of the Services and Performance Indicators, and represents a level of non-performance by the Supplier which would represent a serious Performance Failure

1.10 The Parties acknowledge and agree that not every Performance Indicator has each Severity Level associated with it. The Parties further acknowledge and agree that no Key Performance Indicator shall be modelled in a way which only has a Critical KPI Failure level. For example, a Key Performance Indicator may have a "Minor KPI Failure" Level and a "Critical KPI Failure" level attributed to it, but not a "Critical KPI Failure" level only.

1.11 If the Supplier fails to measure or report on a Performance Indicator in accordance with the requirements placed upon it by Part B of this Schedule, the Supplier shall be deemed to have failed to meet the Target Performance Level for the relevant Performance Indicator in the relevant Measurement Period, unless the Authority otherwise agrees in writing. For the purposes of paragraphs 3 below, Service Points shall accrue to the Supplier in respect of that deemed Performance Failure and following the relevant Service Period at the highest available level associated with that Performance Indicator.

1.12 Service Points, and therefore Service Credits, shall accrue for any KPI Failure which occurs in the relevant Measurement Period and shall be calculated in accordance with Paragraphs 3,4 and 6 of this Part A.

1.13 Service Points do not accrue for any SPI Failure which occurs in the relevant Measurement Period, however the relevant Subsidiary Performance Indicator shall be monitored and reported on in accordance with Part B of this Schedule.

2 CREATION, MODIFICATION, PROMOTION AND DEMOTION OF PERFORMANCE INDICATORS AND KEY BUSINESS EVENTS

2.1 Without prejudice to the rules on promotion and demotion below, new Performance Indicators for existing Services may only be added to the Agreement through the Change Control Procedure. Where a new Service is introduced to this Agreement through the Change Control Procedure, appropriate Performance Indicators, Target Performance Levels Major Failure Performance Thresholds and Critical Failure Performance Thresholds may either be proposed by the Authority or failing that, shall be proposed by the Supplier (acting reasonably and in good faith in accordance with Good Industry Practice) as part of its Impact Assessment in relation to the relevant proposed Change (and, so far as possible, taking an approach which is commensurate with the nearest equivalent Performance Indicator(s) already in existence under the Agreement and the best equivalent level which is otherwise available in the market at the relevant time). Such proposed details will be agreed and documented at the same time that the new Service is agreed and documented. Unless otherwise agreed in writing by the Authority, the Supplier shall not be entitled to invoice for any relevant Run Service Charges for any new Service and the new Service shall not commence until the Performance Indicators, Target Performance Levels Major Failure Performance Thresholds and Critical Failure Performance Thresholds which are to apply to the same have been defined, agreed and documented.

2.2 Once Performance Indicators, Target Performance Levels and Major Failure and Critical Failure Performance Thresholds and Severity Levels have been defined, agreed and documented for a new Service in accordance with paragraph 2.1 above, the Supplier shall be entitled to invoice the Authority in respect of its provision of the new Service from the date on which the new Service commenced. Any such invoice shall take account of and include any Service Credits which would have accrued to the Authority had the new Performance Indicators, Target Performance Levels and Severity Levels (which have been agreed in respect of the relevant Service) been agreed and applicable from and including the date on which the new Service commenced (including deemed failures as provided for in paragraph 1.11 above).

2.3 The Authority may remove a Performance Indicator at its sole discretion at any time by giving notice to the Supplier. Such notice and removal will take effect from the end of the relevant applicable Measurement Period or, if sooner, the date following 30 days from the date of the notice (or such other time, if any, as may be specified by the Authority in the relevant notice). The consequence of such removal by the Authority shall be that the removed Performance Indicator will no longer be applicable to future or existing Services and any Service Points which may have been attributed to such a removed Performance Indicator may be re-allocated by the Authority amongst the remaining Performance Indicators in accordance with paragraph 3.5 below save that such re-allocation may happen at any time in line with, and shall take effect at the same time as, the removal of the relevant Performance Indicator.

2.4 Without prejudice to the ability of the Authority to select between different Service Level Categories and/or any changes in accordance with Paragraphs 2.8 and 2.9 below Target Performance Level, Major Failure Performance Threshold, Critical Failure Performance Threshold, and/or a Severity Level may only be changed as a result of the application of:

(a) the Change Control Procedure;

(b) the continuous improvement requirements set out in clause 8 of this Agreement which will be addressed through the Change Control Procedure;

(c) the agreed results of a benchmarking exercise which is carried out pursuant to the provisions of Schedule 7.3 (*Value for Money*) which will be addressed through the Change Control Procedure; or

(d) an adjustment under paragraphs 2.8 and 2.9 below to reflect the designation by the Authority of a Key Business Event.

2.5 Any KPI may, at any time, be demoted by the Authority to an SPI at the sole discretion of the Authority and by sending written notice to the Supplier. Any such demotion shall take effect from the end of the relevant applicable Measurement Period or, if sooner, the date falling 30 days from the date of the relevant notice (or such other time, if any, as may be specified by the Authority in the relevant notice) . Where a KPI is demoted to a SPI, Service Points shall no longer accrue where the Supplier fails to meet or exceed the Target Performance Level in respect of such Performance Indicator. All other attributes (including the relevant Target Performance Level and Severity Levels) of the KPI shall remain unaffected. Any Service Points which may have been attributed to such a demoted KPI may be re-allocated by the Authority amongst the remaining Performance Indicators in accordance with paragraph 3.5 below, save that such re-allocation may happen at any time and in line with, and shall take effect at the same time as, the demotion of the relevant KPI.

2.6 Subject to the remaining provisions of this paragraph 2.6, and without prejudice (and in addition) to paragraph 2.7 below, a SPI may be promoted to a KPI at the sole discretion of the Authority by sending written notice to the Supplier at least one relevant Measurement Period in advance of any such promotion. The promotion of an SPI to a KPI shall take effect at the start of the next Measurement Period to commence for that promoted SPI following service of notice in writing by the Authority in accordance with this paragraph 2.6. The Parties agree that:

(a) no more than one (1) SPI can be promoted to a KPI per Delivery Group in any one Measurement Period (where relevant, in respect of any one Delivery Group) but without prejudice and in addition to any promotion under paragraph 2.7 below;

(b) no promoted KPI can be demoted to an SPI for three (3) full relevant Measurement Periods (commencing with the first Measurement Period to occur for the new KPI following service of notice in writing by the Authority in accordance with this paragraph 2.6);

(c) promoted KPIs shall be liable to accrue Service Points in accordance with the provisions of paragraph 3 (and the Authority may in the notice of promotion confirm how Service points are to be allocated to the relevant promoted KPI and, where relevant, moves from other KPIs); and

(d) to the extent that it does not already have one, the Authority may designate the Major Failure Performance Threshold(s) and/or Critical Failure Performance Threshold(s) which will apply to the newly promoted KPI

2.7 In addition to any promotion under paragraph 2.6 above, the Authority shall be entitled to promote a SPI to a KPI when the SPI has accrued a Repeat SPI Failure (as further outlined in paragraph 4). Where the relevant SPI is promoted to a KPI (which shall be conducted in accordance with paragraph 2.6), the Repeat Failure Count which applied to the SPI shall be reset to zero (0) (i.e. as if there had been no preceding Performance Failure in respect of the newly promoted KPI).

2.8 With regards to Output Services and Input Services Delivery Group, the Authority may, at any time on 30 days notice in writing to the Supplier, declare that a particular event relating to the business of the Authority and/or any Delivery Group is a Key Business Event ("**KBE Notice**"). In such KBE Notice, the Authority may also set out any adjustments which it requires in relation to the Performance Indicators and which will apply for the purposes of that Key Business Event. Such adjustments and notice may include:

(a) the date on which the adjustments will take effect

(b) NOT USED

(c) the relevant duration for which the adjustments will apply

2.9 In the event that the Authority serves a KBE Notice on the Supplier in accordance with paragraph 2.8 above, the Supplier agrees that the relevant adjustments shall apply to this Schedule for any duration set out in the notice or, if no such duration is specified, until the Authority provides a further notice in writing to the Supplier confirming that the relevant Key Business Event has ended and the relevant adjustments are no longer required ("**KBE End Notice**"). The KBE End Notice shall take effect meaning that the relevant adjustments shall (without prejudice to any Changes to the Agreement which may have been agreed between the Parties following the service of the relevant KBE Notice) cease to apply for the purposes of this Agreement no sooner than 10 days from the date of the relevant KBE End Notice.

3 SERVICE POINTS

3.1 If the level of performance of the Supplier during a Measurement Period meets or exceeds the Target Performance Level in respect of a Key Performance Indicator, no Service Points shall accrue to the Supplier in respect of that Key Performance Indicator.

3.2 If the level of performance of the Supplier during a Measurement Period is below the Target Performance Level in respect of a Key Performance Indicator, Service Points shall accrue to the Supplier in respect of that Key Performance Indicator as set out in Annex 1 (and as such points may be adjusted in accordance with this Schedule).

3.3 The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure shall be the relevant number as set out in Annex 1 (in its form at the relevant time and as may be adjusted in accordance with this Schedule and the Agreement) depending on whether the KPI Failure is a Minor KPI Failure, a Major KPI Failure or a Critical KPI Failure, unless the KPI Failure is a Repeat KPI Failure in which case the provisions of paragraph 4 shall also apply. For the avoidance of doubt, where a KPI only has Service Points associated with a Minor KPI failure and/or a Major KPI Failure, then in the event of a Critical KPI Failure against that KPI, Service Points shall still accrue to the Supplier, and at the highest available amount associated with that KPI.

3.4 It is acknowledged and agreed that the total number of Service Points that may be allocated across all KPIs for a Delivery Group shall not exceed 60. In calculating this figure, the Service Points that are deemed to be allocated to any one KPI shall be the maximum Service Points that can be awarded in respect of a Performance Failure relating to that Key Performance Indicator. Annex 1 to this Schedule sets out the initial allocation of Service Points across the KPIs and shall be updated from time to time in accordance with the provisions of this Schedule.

Example: if, for a particular KPI, a Minor KPI Failure is allocated 5 Service Points and a Major KPI Failure is allocated 10 Service Points, the total Service Point allocation to that KPI for the purposes of this paragraph (and assessing the amount from the total mentioned above which is allocated to that KPI) would be 10.

3.5 The Authority shall be entitled to redistribute Service Points between KPIs (including newly promoted KPIs and from demoted or removed KPIs) at its sole discretion by giving at least one (1) months' notice in writing to the Supplier without prejudice to any time periods applicable under paragraph 2.3, 2.5 or 2.6 above but without having to follow the Change Control Procedure, subject to the following restrictions:

(a) the maximum number of Service Points that can be allocated to any one (1) single KPI is 10 (without prejudice to the application of Paragraph 4 below in relation to Repeat Failures);

(b) no more than 20 Service Points can be reallocated across all of the KPIs per Delivery Group in any one Measurement Period (save for any reallocation as a result of a promotion under paragraph 2.7 above and/or as a result of a Key Business Event as described at paragraphs 2.8 and 2.9 above);

(c) any such reallocation shall take effect at the start of the next Measurement Period to commence for the relevant KPIs following service of notice in writing by the Authority in accordance with this paragraph 3.5; and

(d) the total Service Points per Delivery Group allocated cannot (without prejudice to the application of Paragraph 4 below) exceed the limit specified in paragraph 3.4, although not all Service Points need to be allocated at all times (For example, only and without prejudice to the formality of this section, a KPI which is measured on a monthly basis may have 10 Service Points deducted from it and moved to a KPI which is measured on a quarterly basis. As the KPI measured on a quarterly basis is on a different measurement cycle to the monthly KPI, those Service Points will not be relevant for accrual until the end of the relevant quarterly Measurement Period). Any unallocated Service Points are available to be allocated by the Authority in addition to the limit specified in 3.5(b).

3.6 For the avoidance of doubt:

(a) Service Points will be accrued by the Supplier in relation to each Delivery Group, based on the relevant Performance Failures which have occurred against the Performance Indicators for that Delivery Group; and

(b) Service Points (and accordingly Service Credits) shall be accrued cumulatively by the Supplier where relevant across the Delivery Groups (and for each KPI against which there is a relevant Performance Failure). Service Credits and Service Points accrued by the Supplier for all Performance Failures in a Service Period shall be added together to give the total Service Credit due from the Supplier in respect of that Service Period.

4 REPEAT KPI FAILURES

4.1 If a KPI Failure occurs in respect of the same Key Performance Indicator in any two consecutive Measurement Period, the second and any subsequent such KPI Failure shall be a "**Repeat KPI Failure**", and in addition, if two KPI failures occur in respect of the same Key Performance Indicator in a six-month period, any subsequent failure shall also be a **"Repeat KPI Failure".**

4.2 If a SPI Failure occurs in respect of the same Subsidiary Performance Indicator in any two consecutive Measurements Periods, the second and any subsequent SPI Failure shall be a "**Repeat SPI Failure**". The Supplier shall track and report on the current number of sequential Repeat SPI Failures for each Subsidiary Performance Indicator.

4.3 In each Performance Monitoring Report, the Supplier shall track and report on the current number of sequential Repeat KPI Failures for each KPI (the **"Repeat Failure Count"**). For example, if a KPI Failure has occurred in three (3) sequential Measurement Periods, the Repeat Failure Count will be two (2).

4.4 The Repeat Failure Count shall be a count of the number of sequential Repeat KPI Failures (being failures to meet the relevant Target Performance Levels). The severity of the Performance Failure shall be irrelevant to the Repeat Failure Count. Any Minor KPI Failures, Major KPI Failures and Critical KPI Failures shall each be counted as one increment of the Repeat Failure Count.

4.5 When, in a Measurement Period, a KPI with a Repeat Failure Count above zero (0) meets its Target Performance Level, the Repeat Failure Count shall be reset to zero (0).

4.6 Without prejudice to the Authority's other rights and remedies, there shall be no upper limit to the Repeat Failure Count. However, a Repeat Failure Count of four (4) or more shall be deemed to be a Critical KPI Failure by the Supplier against the relevant KPI.

4.7 The number of Service Points that shall accrue to the Supplier in respect of a Measurement Period and for a KPI Failure that is a Repeat KPI Failure shall be calculated as follows:

SP = P + (P * RFC [* 0.5])

where:

SP = the number of Service Points that shall accrue for the relevant Repeat KPI Failure;

P = the applicable number of Service Points for that KPI Failure as set out in Annex 1 (as updated) depending on whether the relevant Repeat KPI Failure

is a Minor KPI Failure, a Major KPI Failure or a Critical KPI Failure and the applicable Service Level Category; and

RFC = the Repeat Failure Count.

5 REMEDIES

5.1 Without prejudice to the Authority's other rights and remedies in this Agreement, the Parties acknowledge and agree that Critical KPI Failures and Repeat KPI Failures (at the level referred to at paragraph 4.6 above) represent a level of non-performance that would entitle the Authority to invoke its termination rights set out in clause 34.1(b)of this Agreement.

5.2 The Parties agree that Service Credits are a non-exclusive remedy, and shall be without prejudice to any rights or remedies of the Authority under this Agreement or at Law including any entitlement that the Authority may have to damages and/or to terminate.

5.3 The provisions of clause 32 of this Agreement shall apply in respect of any failure by the Supplier to provide the Services in accordance with the Target Performance Levels which would not have occurred but for an Authority Cause.

5.4 Once any necessary allocation of Service Points has been determined and made, the Parties shall make the necessary adjustments to the next invoice to be raised by the Supplier pursuant to Schedule 7.1 (*Charges and Invoicing*).

6 SERVICE CREDITS AND AMOUNT AT RISK

6.1 Schedule 7.1 (*Charges and Invoicing*) sets out the mechanism by which Service Credits are applied to invoices.

6.2 The maximum Service Credits which shall be payable by the Supplier in respect of a failure to meet the relevant Key Performance Indicators relating to a particular Delivery Group, irrespective of the number of Service Points accrued, shall not exceed the Service Credit Cap.

6.3 The Service Credit Cap shall be, **REDACTED**% of the monthly Service Charges for that Delivery Group. For the avoidance of doubt, the operation of a Service Credit Cap shall not affect the continued accrual of Service Points where relevant in accordance with the provisions of this Schedule (for the purposes of calculating whether certain thresholds within this Agreement have been reached).

6.4 Service Credits for a Delivery Group shall be calculated by reference to the number of Service Points accrued in any one Service Period in relation to that Delivery Group and by reference to those Key Performance Indicators for which the Measurement Period ended in or at the end of that Service Period.

6.5 For each Service Period:

(a) the Service Points accrued shall be converted to a percentage deduction from the Service Charges for the relevant Service Period; and

(b) the total Service Credits applicable for a Delivery Group in respect of the Service Period shall be calculated in accordance with the following formula:

SC = TSP *x* X *x* AC

where:

SC is the total Service Credits for the relevant Service Period for the Delivery Group;

TSP is the total Service Points that have accrued for the relevant Service Period for the Delivery Group;

X is 1%;

AC for Input Services and Output Services Delivery Group is the total Service Charges payable for the relevant Service Period for the Delivery Group (prior to deduction of applicable Service Credits). For Email and Mobile Messaging Delivery Group is the total Service Charges for the appropriate individual service line for the relevant Service Period (prior to deduction of applicable Service Credits).

6.6 The Authority shall use the Performance Monitoring Reports provided pursuant to Part B, amongst other things, to verify the calculation and accuracy of the Service Credits (if any) applicable to each Service Period.

6.7 It is acknowledged and agreed that, where in accordance with this Schedule, a change is made to the Performance Indicators, including (but not limited to) a change in the allocation of Service Points and/or the promotion or demotion of a SPI or KPI, the Authority may issue a revised version of Annex 1 reflecting such changes and that version shall, as between the Parties, apply for the purposes of this Schedule from that point.

PART B | PERFORMANCE MONITORING

7 PERFORMANCE MONITORING AND PERFORMANCE REVIEW

7.0 i. Within ten (10) Working Days of the end of each Service Period, the Supplier shall provide:

a. a report to the Authority Representative which summarises the performance by the Supplier against each of the applicable Target Performance Levels as more particularly described in Paragraph 1.2 of this Part B (the **"Performance Monitoring Report"**); and

b. a report created by the Supplier to the Authority's senior responsible officer which summarises the Supplier's performance over the relevant Service Period as more particularly described in Paragraph 1.3 (the **"Balanced Scorecard Report"**).

ii. The Supplier shall carry out and show the performance monitoring and performance review individually for each Delivery Group. The method of performance reporting for each Delivery Group in accordance with this Part B shall be in such format (and using such tools) as the Authority may request from time to time.

7.1 The Performance Monitoring Report shall be in such format as requested by the Authority from time to time, but shall contain, as a minimum, the following information:

Information in respect of the Service Period just ended

(a) for each Key Performance Indicator and Subsidiary Performance Indicator, the actual performance achieved over the Service Period and the relevant Measurement Period which has just ended, and that achieved over the previous three (3) relevant Measurement Periods;

(b) a summary of all Performance Failures that occurred during or which have occurred by the end of the Service Period;

(c) the Severity Level of each Performance Failure which occurred during the Service Period or by the end of it;

(d) which Performance Failures remain outstanding and progress in resolving them;

(e) for any Critical KPI Failures occurring during or by the end of the Service Period, the cause of the relevant KPI Failure and the action being taken to reduce the likelihood of recurrence;

(f) the status of any outstanding Rectification Plan processes, including:

(i) whether or not a Rectification Plan has been agreed; and

(ii) where a Rectification Plan has been agreed, a summary of the Supplier's progress in implementing that Rectification Plan;

(g) for any Repeat KPI Failures and/or Repeat SPI Failures, actions taken to resolve the underlying cause and prevent recurrence;

(h) the number of Service Points awarded in respect of each KPI Failure;

(i) the Service Credits to be applied, indicating the KPI Failure(s) to which the Service Credits relate;

(j) relevant particulars of any aspects of the Supplier's performance which fail to meet the requirements of this Agreement;

(k) such other details as the Authority may reasonably require from time to time;

Information in respect of previous Service Periods

(l) a rolling total of the number of Performance Failures that have occurred over or by the end of the past six Service Periods, including any Repeat Failure Counts; and

(m) the amount of Service Credits that have been incurred by the Supplier over or by the end of the past six Service Periods.

7.2 The Balanced Scorecard Report shall be presented in the form of an online accessible dashboard and, as a minimum, shall contain a high level summary of the Supplier's performance over the relevant Service Period, including details of the following:

(a) financial indicators;

(b) the Target Performance Levels achieved;

(c) behavioural indicators;

(d) performance against its obligation to pay its Sub-contractors within thirty (30) days of receipt of an undisputed invoice;

(e) performance against its obligation to pay its Unconnected Sub-contractors within sixty (60) days of receipt of an invoice;

(f) Milestone trend chart, showing performance of the overall programme;

(g) sustainability and energy efficiency indicators, for example energy consumption and recycling performance; and

(h) Social Value.

Performance Disputes

7.3 The Performance Monitoring Report and the Balanced Scorecard Report shall be reviewed by the Authority including at the next Performance Review Meeting held in accordance with Paragraph 1.5. The Supplier acknowledges and agrees that the Authority may, whilst it considers the Performance Monitoring Report, provide, acting reasonably and in good faith, its own assessment of the Supplier's actual level of performance against a particular Performance Indicator. In the event of any dispute or difference between the Supplier's assessment and the Authority's assessment in respect of a Performance Indicator the Authority's assessment shall, for the purposes of the calculation of the Supplier's level of actual performance in relation to the relevant Measurement Period (and any associated remedies) prevail. However, without prejudice to the foregoing, the Supplier shall be entitled to subsequently escalate any remaining dispute or difference in accordance with Schedule 8.4 (*Dispute Resolution*).

7.4 The Parties shall attend meetings on a monthly basis (unless otherwise agreed) to review the Performance Monitoring Reports and the Balanced Scorecard Reports. These meetings ("**Performance Review Meetings**") shall (unless otherwise agreed):

(a) take place within five (5) Working Days of the Performance Monitoring Report being issued by the Supplier;

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

(c) be attended by the Supplier Representative and the Authority Representative.

7.5 The Authority shall be entitled to raise any additional questions and/or request any further information from the Supplier regarding any Performance Failure.

7.6 In addition to the requirements above and elsewhere in this Agreement to maintain and provide appropriate documents and records, the Supplier 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 Supplier both before and after each Operational Service Date.

7.7 The Supplier shall ensure that the Performance Monitoring Report, the Balanced Scorecard Report (as well historic Performance Monitoring Reports and historic Balance Scorecard Reports) and any variations or amendments thereto, any reports and summaries produced in accordance with this Schedule and any other document or record reasonably required by the Authority are available to the Authority on-line and are capable of being printed.

8 PERFORMANCE VERIFICATION

The Authority reserves the right to verify any aspect of the Services and the Supplier's performance under this Agreement against the Target Performance Levels, including by sending test transactions through the IT Environment or otherwise.

PART II: Performance Indicator Specific Definitions

NOT USED

HM Revenue & Customs

HMRC Tier 1 and 2 Model ICT Contract
Version 2.3 (December 2020)

SCHEDULE 2.3 | Standards

Schedule 2.3 | Standards

1. DEFINITIONS

In this Schedule, the following definitions shall apply:

"Standards Hub"	the Government's open and transparent standards adoption process as documented at http://standards.data.gov.uk/; and
"Suggested Challenge"	a submission to suggest the adoption of new or emergent standards in the format specified on Standards Hub.

2. GENERAL

2.1 Throughout the term of this Agreement, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier's provision, or the Authority's receipt, of the Services. Any changes to the Standards, including the adoption of any such new or emergent standard, shall be agreed in accordance with the Change Control Procedure.

2.2 Where a new or emergent standard is to be developed or introduced by the Authority, the Supplier shall be responsible for ensuring that the potential impact on the Supplier's provision, or the Authority's receipt, of the Services is explained to the Authority (within a reasonable timeframe), prior to the implementation of the new or emergent standard.

2.3 Where Standards referenced conflict with each other or with Good Industry Practice, then the Supplier shall escalate details of the conflict through the governance process set out in Schedule 8.1 (Governance) providing all information required to enable the Authority to make an informed decision. Any such alteration to any Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

3. TECHNOLOGY AND DIGITAL SERVICES PRACTICE

The Supplier shall (when designing, implementing and delivering the Services) adopt the applicable elements of HM Government's Technology Code of Practice as documented at https://www.gov.uk/service-manual/technology/code-of-practice.html.

4. OPEN DATA STANDARDS & STANDARDS HUB

4.1 The Supplier shall comply to the extent within its control with UK Government's Open Standards Principles as documented at

https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles, as they relate to the specification of standards for software interoperability, data and document formats in the IT Environment.

4.2 Without prejudice to the generality of Paragraph 2.2, the Supplier shall, when implementing or updating a technical component or part of the Software or Supplier Solution where there is a requirement under this Agreement or opportunity to use a new or emergent standard, submit a Suggested Challenge compliant with the UK Government's Open Standards Principles (using the process detailed on Standards Hub and documented at http://standards.data.gov.uk/). Each Suggested Challenge submitted by the Supplier shall detail, subject to the security and confidentiality provisions in this Agreement, an illustration of such requirement or opportunity within the IT Environment, Supplier Solution and Government's IT infrastructure and the suggested open standard.

4.3 The Supplier shall ensure that all documentation published on behalf of the Authority pursuant to this Agreement is provided in a non-proprietary format (such as PDF or Open Document Format (ISO 26300 or equivalent)) as well as any native file format documentation in accordance with the obligation under Paragraph 4.1 to comply with the UK Government's Open Standards Principles, unless the Authority otherwise agrees in writing.

5. TECHNOLOGY ARCHITECTURE STANDARDS

The Supplier shall produce full and detailed technical architecture documentation for the Supplier Solution in accordance with Good Industry Practice. If documentation exists that complies with the Open Group Architecture Framework 9.2 or its equivalent, then this shall be deemed acceptable.

6. ACCESSIBLE DIGITAL STANDARDS

The Supplier shall comply with (or with equivalents to):

(a) the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.1 Conformance Level AA; and

(b) ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability.

7. SERVICE MANAGEMENT SOFTWARE & STANDARDS

7.1 Subject to Paragraphs 2 to 4 (inclusive), the Supplier shall reference relevant industry and HM Government standards and best practice guidelines in the management of the Services, including the following and/or their equivalents:

(a) ITIL v4;

(b) ISO/IEC 20000-1 2018 “Information technology — Service management – Part 1”;

(c) ISO/IEC 20000-2 2019 “Information technology — Service management – Part 2”;

(d) ISO 10007: 2017 “Quality management systems – Guidelines for configuration management”;

(e) ISO 22313:2020 “Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301” and, ISO/IEC 27031:2011 and ISO 22301; and

(f) BS10008 Evidential Weight and Legal Admissibility of Electronic Information.

7.2 For the purposes of management of the Services and delivery performance the Supplier shall make use of Software that complies with Good Industry Practice including availability, change, incident, knowledge, problem, release & deployment, request fulfilment, service asset and configuration, service catalogue, service level and service portfolio management. If such Software has been assessed under the ITIL Software Scheme as being compliant to “Bronze Level”, then this shall be deemed acceptable.

7.3 The Supplier shall comply with and feed into the Authority's incident and problem management processes and procedures.

8. ENVIRONMENTAL STANDARDS

8.1 The Supplier shall comply with the environmental requirements set out in the Annex to this Schedule.

9. HARDWARE SAFETY STANDARDS

9.1 The Supplier shall comply with those BS or other standards relevant to the provision of the Services, including the following or their equivalents:

(a) any new hardware required for the delivery of the Services (including printers), shall conform to BS EN IEC 62368-1:2020+A11:2020 or subsequent replacements. In considering where to site any such hardware, the Supplier shall consider the future working user environment and shall position the hardware sympathetically, wherever possible;

(b) any new audio, video and similar electronic apparatus required for the delivery of the Services, shall conform to the following standard: BS EN IEC 62368-1:2020+A11:2020 or any subsequent replacements;

(c) any new laser printers or scanners using lasers, required for the delivery of the Services, shall conform to either of the following safety Standards: BS EN 60825-1:2014 or any subsequent replacements; and

(d) any new apparatus for connection to any telecommunication network, and required for the delivery of the Services, shall conform to the following safety Standard: BS EN 62949:2017 or any subsequent replacements.

Where required to do so as part of the Services, the Supplier shall perform electrical safety checks in relation to all equipment supplied under this Agreement in accordance with the relevant health and safety regulations.

10. SECURITY STANDARDS

10.1 The Supplier shall comply with the security requirements stipulated by the Authority in Schedule 2.4 (*Security Management*) which shall, as a minimum, be ISO27001 and the government sponsored cyber essentials, (or their equivalent).

ANNEX 1 ENVIRONMENTAL REQUIREMENTS

1 DEFINITIONS

1.1 In this Annex, the following definitions shall apply:

"Permitted Item"	means those items which are permissible under this Agreement to the extent set out in Table B of this Annex
"Prohibited Items"	means those items which are not permissible under this Agreement as set out at Table A of this Annex
"Sustainability Reports"	written reports to be completed by the Supplier containing the information outlined in Table C of this Annex
"Waste Hierarchy"	means prioritisation of waste management in the following order of preference:

(a) Prevention – by using less material in design and manufacture. Keeping products for longer;

(b) Preparing for re-use – by checking, cleaning, repairing, refurbishing, whole items or spare parts;

(c) Recycling – by turning waste into a new substance or produce, including composting if it meets quality protocols;

(d) Other Recovery – through anaerobic digestion, incineration with energy recovery, gasification and pyrolysis which produce energy (fuels, heat and power) and materials from waste; some backfilling; and

(e) Disposal - Landfill and incineration without energy recovery.

2 ENVIRONMENTAL REQUIREMENTS

2.1 The Supplier shall comply in all material respects with all applicable environmental laws and regulations in force in relation to the Agreement.

2.2 The Supplier warrants that it has obtained ISO 14001 certification from an accredited body and shall comply with and maintain certification requirements throughout the Term.

2.3 In performing its obligations under the Agreement, the Supplier shall to the reasonable satisfaction of the Authority:

(a) demonstrate low carbon resource efficiency, including minimising the use of resources and responding promptly to the Authority's reasonable questions;

(b) prioritise waste management in accordance with the Waste Hierarchy;

(c) be responsible for ensuring that any waste generated by the Supplier and sent for recycling, disposal or other recovery as a consequence of this Agreement is taken to an authorised site for treatment or disposal and that the disposal or treatment of waste complies with the law;

(d) ensure that it and any third parties used to undertake recycling disposal or other recovery as a consequence of this Agreement do so in a legally compliant way, undertake reasonable checks on a regular basis to ensure this;

(e) inform the Environmental Agency within one Working Day in the event that a permit or exemption to carry or send waste generated under this Agreement is revoked and in circumstances where a permit or exemption to carry or send waste generated under this Agreement is revoked the Supplier shall cease to carry or send waste or allow waste to be carried by any Sub-contractor until authorisation is obtained from the Environmental Agency;

(f) minimise the release of greenhouse gases (including carbon dioxide emissions), air pollutants, volatile organic compounds and other substances damaging to health and the environment; and

(g) reduce and minimise carbon emissions by taking into account factors including, but not limited to, the locations from which materials are sourced, the transport of materials, the locations from which the work force are recruited and emissions from offices and on-site equipment.

2.4 The Supplier shall use reasonable endeavours to avoid the use of paper and card in carrying out its obligations under this Agreement. Where unavoidable under reasonable endeavours, the Supplier shall ensure that any paper or card deployed in the performance of the Services consists of at least seventy-five percent (75%) recycled content and used on both sides where feasible to do so. This Paragraph 2.4 shall not apply when

printing outbound mail. For the avoidance of doubt, in the event of any conflict or inconsistency between this Paragraph 2.4 and the provisions of Schedule 2.1 (Services Description), the provisions of Schedule 2.1 shall prevail (as per the order of precedence in Clause 1.4 of the Terms and Conditions).

2.5 The Supplier shall not provide to the Authority Goods or Deliverables which comprise wholly or partly of Prohibited Items unless such item is a Permitted Item.

2.6 The Supplier shall not use anything which comprises wholly or partly of the Prohibited Items to provide the Services under this Agreement unless:

(a) it is a Permitted Item; or

(b) the use is primarily related to the management of the Supplier's own facilities or internal operations as opposed to the provision of Services.

2.7 The Supplier shall complete the Sustainability Report in relation its provision of the Services under this Agreement and provide the Sustainability Report to the Authority on the date and frequency outlined in Table C of this Annex.

2.8 The Supplier shall comply with reasonable requests by the Authority for information evidencing compliance with the provisions of this Annex within fourteen (14) days of such request, provided that such requests are limited to two per Contract Year.

2.9 In performing its obligations under the Agreement, the Supplier shall to the reasonable satisfaction of the Authority (where the anticipated Charges in any Contract Year are above £5 million per annum (excluding VAT)), where related to and proportionate to the contract in accordance with PPN 06/21), publish and maintain a credible Carbon Reduction Plan in accordance with PPN 06/21.

TABLE A – Prohibited Items

The following consumer single use plastics are Prohibited Items:	**Catering** a. Single use sachets e.g., coffee pods, sauce sachets, milk sachets b. Take away cutlery c. Take away boxes and plates d. Cups made wholly or partially of plastic e. Straws f. Stirrers g. Water bottles
	Facilities a. Single use containers e.g., hand soap, cleaning products b. Wipes containing plastic
	Office Supplies a. Plastic envelopes b. Plastic wrapping for brochures c. Paper or card which is bleached with chlorine
	Packaging a. Single use plastic packaging from deliveries where avoidable e.g., shrink wrapped packaging from office supplier or facilities products. b. Single use carrier bags
Authority specific Prohibitions	*N/A*

Project specific Prohibitions	*N/A*

TABLE B – Permitted Items

Authority Permitted Items	*N/A*
Project Specific Permitted Items	*N/A*

TABLE C – Sustainability Reports

Report Name	Content of Report	Frequency of Report
Sustainability Impact	a. the key sustainability impacts identified; b. sustainability improvements made; c. actions underway or planned to reduce sustainability impacts; d. contributions made to the Authority's sustainability policies and objectives; e. sustainability policies, standards, targets and practices that have been adopted to reduce the environmental impact of the Supplier's operations and evidence of these being actively pursued, indicating arrangements for engagement and achievements. This can also include where positive sustainability impacts have been delivered; and f. risks to the Service and Subcontractors of climate change and severe weather events such as flooding and extreme temperatures including mitigation, adaptation and continuity plans employed by the Supplier in response to those risks.	On the anniversary of the Effective Date
Waste created	By type of material the weight of waste categories by each means of disposal in the Waste Hierarchy with separate figures for disposal by incineration and landfill.	Before contract award and on the anniversary of the Effective Date.
Waste permits	Copies of relevant permits and exemptions for waste, handling, storage and disposal.	Before the Effective Date, on the anniversary of the Effective Date and within ten (10) Working Days of there is any change or renewal to license or

		exemption to carry, store or dispose waste
Greenhouse Gas Emissions	Indicate greenhouse gas emissions making use of the use of the most recent conversion guidance set out in 'Greenhouse gas reporting – Conversion factors' available online at https://www.gov.uk/guidance/measuring-and-reporting-environmental-impacts-guidance-for-businesses	On the anniversary of the Effective Date
Water Use	Volume in metres cubed.	On the anniversary of the Effective Date
Energy Use	Separate energy consumption figures for: a. assets deployed on the Supplier's site; b. assets deployed on the Authority's site; c. assets deployed off-site; and d. energy consumed by IT assets and by any cooling devices deployed. Power Usage Effectiveness (PUE) rating for each data centre/server room in accordance with ISO/IEC 31034-2/EN 50600-4-2.	On the anniversary of the Effective Date
Transport Use	a. miles travelled by transport and fuel type, for goods delivered to the Authority's sites; b. miles travelled by staff when visiting the Authority's sites from the Supplier's sites or home; c. resulting Green House Gas (GHG) emissions using agreed Conversion Factors; and d. the number of multi-lateral e-meetings i.e., with more than two attendees, held by type (audio,	on the anniversary of the Effective Date

	webinar, v/conferencing) their length and number of attendees	
Materials	Materials usage, including: a. type of material used; b. quantity or volume of material used; and c. amount of recycled/recovered material used	

HM Revenue & Customs

HMRC Tier 1 and 2 Model ICT Contract
Version 2.3 (December 2020)

SCHEDULE 2.4 | Security Management

Schedule 2.4 | Security Management

1 DEFINITIONS

In this Schedule, the following definitions shall apply:

"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and/or any IT, information or data (including the Confidential Information and the Authority Data) used by the Authority and/or the Supplier in connection with this Agreement; and/or (b) the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including any copies of such information or data, used by the Authority and/or the Supplier in connection with this Agreement; and/or (c) a failure to comply with the personnel security requirements, as set out in the Security Management Plan, in either case as more particularly set out in the Security requirements in Schedule 2.1 (*Services Description*) and the Baseline Security Requirements;
"CCP"	CESG Certified Practitioner;
"CESG"	the UK Government's national technical authority for information assurance;
"CHECK Scheme"	The scheme for penetration testing of data processing systems operated by the CESG;
"CPA"	the CESG Commercial Product Assurance scheme;
"CPNI"	Centre for Protection of National Infrastructure;
"ISMS"	the information security management system and processes developed by the Supplier in accordance

	with Paragraph 3 as updated from time to time in accordance with this Schedule;
"Security Policy Framework"	the Security Policy Framework published by the Cabinet Office as updated from time to time including any details notified by the Authority to the Supplier;
"Security Management Plan"	is the document produced by the Supplier, a copy of which is at Annex 2;
"Security Questionnaire"	the questionnaire produced by the Authority which, when completed by the Supplier, will form the basis of the Supplier's Security Management Plan; and
"Security Tests"	tests carried out where relevant in accordance with the CHECK Scheme or to an equivalent standard to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

2 INTRODUCTION

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

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

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

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

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

2.6 The Supplier's own security policy should align with the contents of the Security Management Plan and incorporate CESG and CPNI best practice.

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

3 ISMS

3.1 By the date specified in the Implementation Plan the Supplier shall develop and submit to the Authority for the Authority's approval in accordance with Paragraph 3.6 an ISMS (information security management system) for the purposes of this Agreement, which:

(a) shall have been tested in accordance with Schedule 6.2 (*Testing Procedures*); and

(b) shall comply with the requirements of Paragraphs 3.3 to 3.5.

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

3.3 The ISMS shall:

(a) unless otherwise specified by the Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement;

(b) meet the relevant requirements in ISO/IEC 27001 and ISO/IEC 27002 in accordance with Paragraph 7; and

(c) at all times provide a level of security which:

(i) is in accordance with Law and this Agreement;

(ii) as a minimum demonstrates Good Industry Practice;

(iii) complies with the Baseline Security Requirements;

(iv) addresses issues of incompatibility with the Supplier's own organisational security policies;

(v) meets any specific security threats of immediate relevance to the Services and/or Authority Data;

(vi) complies with the security requirements as set out in Schedule 2.1 (*Services Description*);

(vii) complies with the Authority's IT policies; and

(viii) is in accordance with the Security Policy Framework.

(d) document the security incident management processes and incident response plans;

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

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

3.4 Subject to Clause 20 (*Authority Data and Security Requirements*) the references to standards, guidance and policies set out in Paragraph 3.3 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.5 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.3, the Supplier shall immediately notify the Authority Representative of such inconsistency and the Authority Representative shall, as soon as practicable, notify the Supplier which provision the Supplier shall comply with.

3.6 If the ISMS submitted to the Authority pursuant to Paragraph 3.1 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not approved by the Authority, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.3 to 3.5 shall be deemed to be reasonable.

3.7 Approval by the Authority of the ISMS pursuant to Paragraph 3.6 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4 SECURITY MANAGEMENT PLAN

4.1 Within twenty (20) Working Days after the Effective Date, the Supplier shall prepare and submit to the Authority for approval in accordance with Paragraph 4.3 a fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

(a) be based on the Supplier's final response to the Authority's Security Questionnaire;

(b) comply with the Baseline Security Requirements set out in Annex 1;

(c) identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

(d) detail the process for vetting staff at the appropriate security level with reference to the level of access staff will have to Authority Data, managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Services, processes associated with the delivery of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;

(e) unless otherwise specified by the Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

(f) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Schedule (including the requirements set out in Paragraph 3;

(g) demonstrate that the Supplier Solution has minimised the Authority and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offerings from the G-Cloud catalogue);

(h) set out the plans for transiting all security arrangements and responsibilities from those in place at the Effective Date to those incorporated in the ISMS at the date set out in Schedule 6.1 (*Transition*) for the Supplier to meet the full obligations of the security requirements set out in Schedule 2.1 (*Services Description*) and this Schedule;

(i) set out the scope of the Authority System that is under the control of the Supplier;

(j) be structured in accordance with ISO/IEC 27001 and ISO/IEC 27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards;

(k) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Authority engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule; and

(l) be in accordance with the Security Policy Framework.

4.3 If the Security Management Plan submitted to the Authority Representative pursuant to Paragraph 4.1 is approved by the Authority Representative, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Authority Representative, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Authority and re-submit it to the Authority Representative for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and, in any event, no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority Representative. If the Authority Representative does not approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority Representative pursuant to this Paragraph 4.3 may be unreasonably withheld or delayed. However, any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

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

5 AMENDMENT AND REVISION OF THE ISMS AND SECURITY MANAGEMENT PLAN

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier within ten (10) Working Days of any Breach of Security and further at least annually to reflect:

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the IT Environment, the Services and/or associated processes;

(c) any new perceived or changed security threats; and

(d) any reasonable change in requirement requested by the Authority.

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

(a) suggested improvements to the effectiveness of the ISMS;

(b) updates to the risk assessments;

(c) proposed modifications to respond to events that may impact on the ISMS including the security incident management process, incident response plans and general procedures and controls that affect information security; and

(d) suggested improvements in measuring the effectiveness of controls.

5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, an Authority request, a change to Schedule 2.1 (*Services Description*) or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Authority.

5.4 The Authority may, where it is reasonable to do so, approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Agreement.

6 SECURITY TESTING

6.1 The Supplier shall conduct relevant Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after significant architectural changes to the IT Environment or after any change or amendment to the ISMS, (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. The Supplier shall conduct, document and provide to the Authority a risk assessment to enable the Authority to consider whether a Security Test should be carried out. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Target Performance Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

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

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

6.4 Where any Security Test carried out pursuant to Paragraphs 6.1 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Authority's prior written approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Baseline Security Requirements or security requirements (as set out in Schedule 2.1 (*Services Description*)) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Authority.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default for the purposes of Clause 27 (*Rectification Plan Process*).

7 ISMS COMPLIANCE

7.1 The Authority shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001, the specific security requirements set out in Schedule 2.1 (*Services Description*) and the Baseline Security Requirements.

7.2 If, on the basis of evidence provided by such audits, it is the Authority's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001, the specific security requirements set out in Schedule 2.1 (*Services Description*) and/or the Baseline Security Requirements is not being achieved by the Supplier, then the Authority shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement any necessary remedy. If the Supplier does not become compliant within the required time, then the Authority shall have the right to obtain an independent audit against these standards in whole or in part. The Supplier shall reimburse in full the costs incurred by the Authority in obtaining such audit.

7.3 If, as a result of any such independent audit as described in Paragraph 7.2 the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001, the specific security requirements set out in Schedule 2.1 (*Services Description*) and/or the Baseline Security Requirements then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and, (as said above), shall reimburse in full the costs incurred by the Authority in obtaining such audit.

8 BREACH OF SECURITY

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

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

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

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

(ii) remedy such Breach of Security to the extent possible and protect the integrity of the IT Environment to the extent within its control against any such Breach of Security or attempted Breach of Security;

(iii) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet the Target Performance Levels, the Supplier shall be granted relief against any resultant under-performance for such period as the Authority, acting reasonably, may specify by written notice to the Supplier;

(iv) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure; and

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

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

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Baseline Security Requirements or security requirements (as set out in Schedule 2.1 (*Services Description*)) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Authority.

9 VULNERABILITES AND CORRECTIVE ACTION

9.1 The Authority and the Supplier acknowledge that from time-to-time vulnerabilities in the IT Environment will be discovered which unless mitigated will present an unacceptable risk to the Authority Materials.

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

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

(b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two (2) remaining levels ('Moderate' and 'Low') respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities (whether such patches are entirely related to security or related in part to security) within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within fourteen (14) days of release, 'Important' within thirty (30) days of release and all 'Other' within sixty (60) Working Days of release, except where:

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

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

(c) the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Supplier Solution and Implementation Plan shall include provisions for major version upgrades of all Supplier Software and Third-Party Software to be upgraded within six (6) months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

(a) where upgrading such Supplier Software and Third-Party Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within twelve (12) months of release of the latest version; or

(b) is agreed with the Authority in writing.

9.5 The Supplier shall:

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

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

(c) ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the IT Environment by actively monitoring the threat landscape during the Term;

(d) pro-actively scan the IT Environment (to the extent that the IT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3(e);

(e) from the date specified in the Security Management Plan (and before the first Operational Service Commencement Date) provide a report to the Authority within five (5) Working Days of the end of each month detailing both patched and outstanding vulnerabilities in the IT Environment (to the extent that the IT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

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

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

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

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

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

ANNEX 1 | Baseline Security Requirements

1 Higher Classifications

1.1 Prior to enabling the Supplier to have access to such SECRET or TOP SECRET information, the Authority shall provide the Supplier with specific guidance regarding how the information is to be handled, and prior to handling such information the Supplier shall seek additional specific guidance from the Authority if no specific guidance has been received from the Authority prior to receipt.

2 End User Devices

2.1 When Authority Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the CESG to at least Foundation Grade, for example, under CPA.

2.2 Devices used to access or manage Authority Data and services must be under the management authority of Authority or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Authority. Unless otherwise agreed with the Authority in writing, all Supplier devices are expected to meet the set of security requirements set out in the CESG End User Devices Platform Security Guidance:

(https://www.gov.uk/government/collections/end-user-devices-security-guidance--2).

As a minimum, the security standards must include Assurance Framework, Ten Critical Steps and Requirements. Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the CESG guidance, then this should be agreed in writing on a case-by-case basis with the Authority.

3. Data Processing, Storage, Management and Destruction

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

3.2 Not Used

3.3 The Supplier shall:

(a) provide the Authority with all Authority Data on demand in an agreed open format;

(b) have documented processes to guarantee availability of Authority Data in the event of the Supplier ceasing to trade;

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

(d) securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority.

4. Networking

4.1 The Authority requires that any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA or through the use of pan-government accredited encrypted networking services via the Public Sector Network ("PSN") framework (which makes use of Foundation Grade certified products).

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

5. Security Architectures

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

5.2 When designing and configuring the IT Environment (to the extent that the IT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (http://www.cesg.gov.uk/awarenesstraining/IA-certification/Pages/index.aspx) for all bespoke or complex components of the Supplier Solution.

6. Personnel Security

6.1 Supplier Personnel shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work (including nationality and immigration status).

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

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

6.4 All Supplier Personnel that have the ability to access Authority Data or systems holding Authority Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Authority in writing, this training must be undertaken annually.

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

6.6 Notwithstanding the Supplier's obligation to ensure that the Security Management Plan is implemented and followed, the Supplier shall ensure that the Supplier Personnel are promptly informed of action taken in relation to any failure to do so.

6.7 The Supplier shall ensure that Supplier Personnel complete the security questionnaire as provided by the Authority from time to time.

6.8 The Supplier shall perform the Off-Shore Personnel Security Checks in relation to any proposed Off-Shore Personnel prior to their engagement to the reasonable satisfaction of the Authority in the delivery of the Services under this Agreement.

7. Identity, Authentication and Access Control

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

8. Audit and Monitoring

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

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

(b) Security events generated in the IT Environment (to the extent that the IT Environment is within the control of the Supplier) and shall include: privileged account logon and logoff events; the start and termination of remote access sessions; security alerts from desktops and server operating systems; and security alerts from third party security software.

8.2 The Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the IT Environment.

8.3 The Supplier shall retain audit records collected in compliance with Paragraph 7.1 for a period of at least six (6) months.

ANNEX 2| Security Management Plan

REDACTED

HM Revenue & Customs

HMRC Tier 1 and 2 Model ICT Contract
Version 2.3 (December 2020)

SCHEDULE 2.5 | Insurance Requirements

Schedule 2.5 | Insurance Requirements

1 OBLIGATION TO MAINTAIN INSURANCES

1.1 Without prejudice to its obligations to the Authority under this Agreement, including its indemnity and liability obligations, the Supplier shall, for the periods specified in this Schedule, take out and maintain, or procure the taking out and maintenance of the insurances as set out in Annex 1 and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than the date on which the relevant risk commences.

1.2 The Insurances shall be maintained in accordance with Good Industry Practice and (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time.

1.3 The Insurances shall be taken out and maintained with insurers who are:

(a) of good financial standing;

(b) appropriately regulated; and

(c) regulated by the applicable regulatory body and is in good standing with that regulator;

(d) of good repute in the international insurance market

1.4 The Supplier shall ensure that the public and products liability policy that it has or puts in place shall contain an indemnity to principal clause under which the Authority shall be indemnified in respect of claims made against the Authority in respect of death or bodily injury or third-party property damage arising out of or in connection with the Agreement and for which the Supplier is legally liable.

2 GENERAL OBLIGATIONS

Without limiting the other provisions of this Agreement, the Supplier shall:

(a) take or procure the taking of all reasonable risk management and risk control measures in relation to the Services as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

(b) promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

(c) hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3 FAILURE TO INSURE

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase any of the Insurances or maintain any of the Insurances in full force and effect, the Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances, and the Authority shall be entitled to recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4 EVIDENCE OF INSURANCES

The Supplier shall upon the Effective Date and within fifteen (15) Working Days after the renewal or replacement of each of the Insurances, provide evidence, in a form satisfactory to the Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule. Receipt of such evidence by the Authority shall not in itself constitute acceptance by the Authority or relieve the Supplier of any of its liabilities and obligations under this Agreement.

5 AGGREGATE LIMIT OF INDEMNITY

Where the minimum limit of indemnity required in relation to any of the Insurances is specified as being "in the aggregate":

(a) if a claim or claims which do not relate to this Agreement are notified to the insurers which, given the nature of the allegations and/or the quantum claimed by the third party(ies), is likely to result in a claim or claims being paid by the insurers which could reduce the level of cover available below that minimum, the Supplier shall immediately submit to the Authority:

(i) details of the policy concerned; and

(ii) its proposed solution for maintaining the minimum limit of indemnity specified; and

(b) if and to the extent that the level of insurance cover available falls below that minimum because a claim or claims which do not relate to this Agreement are paid by insurers, the Supplier shall:

(i) ensure that the insurance cover is reinstated to maintain at all times the minimum limit of indemnity specified for claims relating to this Agreement; or

(ii) if the Supplier is or has reason to believe that it will be unable to ensure that insurance cover is reinstated to maintain at all times the minimum limit of indemnity specified, immediately submit to the Authority full

details of the policy concerned and its proposed solution for maintaining the minimum limit of indemnity specified.

6 CANCELLATION, SUSPENSION, TERMINATION OR NON-RENEWAL

6.1 Subject to Paragraph 6.2, the Supplier shall notify the Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination, or non-renewal of any of the Insurances.

6.2 Without prejudice to the Supplier's obligations under Paragraph 4, Paragraph 6.1 shall not apply where the termination of any Insurances occurs purely as a result of a change of insurer in respect of any of the Insurances required to be taken out and maintained in accordance with this Schedule.

7 INSURANCE CLAIMS

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Services and/or this Agreement for which it may be entitled to claim under any of the Insurances. In the event that the Authority receives a claim relating to or arising out of the Services and/or this Agreement, the Supplier shall co-operate with the Authority and assist it in dealing with such claims at its own expense including without limitation providing information and documentation in a timely manner.

7.2 The Supplier shall maintain a register of all claims under the Insurances in connection with this Agreement and shall allow the Authority to review such register at any time.

7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Agreement or otherwise.

ANNEX 1 | Required Insurances

PART A: INSURANCE CLAIM NOTIFICATION

Except where the Authority is the claimant party, the Supplier shall give the Authority notice within twenty (20) Working Days after any insurance claim in excess of £100,000 relating to or arising out of the provision of the Services or this Agreement on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Authority) full details of the incident giving rise to the claim.

PART B: THIRD PARTY PUBLIC AND PRODUCTS LIABILITY INSURANCE

1 Insured

The Supplier

2 Interest

To indemnify the Insured in respect of all sums which the Insured shall become legally liable to pay as damages, including claimant's costs and expenses, in respect of accidental:

(a) death or bodily injury to or sickness, illness or disease contracted by any person; and

(b) loss of or damage to property;

happening during the period of insurance (as specified in Paragraph 5) and arising out of or in connection with the provision of the Services and in connection with this Agreement.

3 Limit of indemnity

Not less than ***£5,000,000 (five million pounds)*** in respect of any one occurrence, the number of occurrences being unlimited in any annual policy period, but ***£15,000,000 (fifteen million pounds)*** in the aggregate per annum in respect of products and pollution liability.

4 Territorial limits

United Kingdom

5 Period of insurance

From the date of this Agreement for the Term and renewable on an annual basis unless agreed otherwise by the Authority in writing.

6 Cover features and extensions

Indemnity to principal clause under which the Authority shall be indemnified in respect of claims made against the Authority in respect of death or bodily injury or third-party property damage arising out of or in connection with the Agreement and for which the Supplier is legally liable.

7 Principal exclusions

7.1 War and related perils.

7.2 Nuclear and radioactive risks.

7.3 Liability for death, illness, disease or bodily injury sustained by employees of the Insured during the course of their employment.

7.4 Liability arising out of the use of mechanically propelled vehicles whilst required to be compulsorily insured by applicable Law in respect of such vehicles.

7.5 Liability in respect of predetermined penalties or liquidated damages imposed under any contract entered into by the Insured.

7.6 Liability arising out of technical or professional advice other than in respect of death or bodily injury to persons or damage to third party property.

7.7 Liability arising from the ownership, possession or use of any aircraft or marine vessel.

7.8 Liability arising from seepage and pollution unless caused by a sudden, unintended and unexpected occurrence.

8 Maximum deductible threshold

Not to exceed £1,000,000 for each and every third-party property damage claim (personal injury claims to be paid in full).

PART C: PROFESSIONAL INDEMNITY INSURANCE

1 Insured

The Supplier

2 Interest

To indemnify the Insured for all sums which the Insured shall become legally liable to pay (including claimants' costs and expenses) as a result of claims first made against the Insured during the period of insurance (as specified in paragraph 5) by reason of any negligent act, error and/or omission arising from or in connection with the provision of the Services.

3 Limit of indemnity

Not less than £*5,000,000 (five million pounds)* in respect of any one claim, the number of claims being unlimited, *but* £15,000,000 (*fifteen million pounds*) in the aggregate per annum, exclusive of defence costs which are payable in addition.

4 Territorial Limits

United Kingdom

5 Period of insurance

From the date of this Agreement and renewable on an annual basis unless agreed otherwise by the Authority in writing (a) throughout the Term or until earlier termination of this Agreement and (b) for a period of six (6) years thereafter.

6 Cover features and extensions

Retroactive cover to apply to any "claims made policy wording" in respect of this Agreement or retroactive date to be no later than the Effective Date.

7 Principal exclusions

7.1 War and related perils

7.2 Nuclear and radioactive risks

8 Maximum deductible threshold

Not to exceed £1,000,000 for each and every claim.

PART D: UNITED KINGDOM COMPULSORY INSURANCES

The Supplier shall meet its insurance obligations under applicable Law in full, including, UK employers' liability insurance and motor third party liability insurance.

HM Revenue & Customs

HMRC Tier 1 and 2 Model ICT Contract
Version 2.3 (December 2020)

SCHEDULE 2.6 | Accommodation

SCHEDULE 2.6 | Accommodation

Property requirements will be addressed on a project-by-project basis. If the Supplier has a requirement to occupy Property and this can be accommodated by HMRC it is most likely that the occupation of the Property will be structured by way of a licence to occupy the terms of which will be tailored to the Property in question and the nature of the occupation.

HM Revenue & Customs

HMRC Tier 1 and 2 Model ICT Contract
Version 2.3 (December 2020)

SCHEDULE 2.7 | Service Recipients and Service Beneficiaries

Schedule 2.7 | Service Recipients and Service Beneficiaries

1 INTRODUCTION

1.1 This Schedule lists:

(a) the Service Recipients to which the Supplier has agreed that it shall provide Services in accordance with Clause 44.5 of this Agreement; and

(b) the Service Beneficiaries that shall be entitled to benefit from the Services provided pursuant to this Agreement.

1.2 The Parties acknowledge and agree that this Schedule may be updated from time to time, pursuant to the Change Control Procedure, in order to:

(a) add additional Service Recipients and/or Service Beneficiaries; or

(b) remove Service Recipients and/or Service Beneficiaries.

2 SERVICE RECIPIENTS

1.	**Name of Service Recipient:**	**[*Insert name of Service Recipient*]**	
	Service line	**Service Description**	**Charging reference**
	[***insert relevant details***]	[***insert relevant details***]	[***insert relevant details***]
	Elements of Service	**Business requirement**	**HMRC Responsibility**

2.	**Name of Service Recipient:**	**[*Insert name of Service Recipient*]**	
	Service line	**Service Description**	**Charging reference**
	[***insert relevant details***]	[***insert relevant details***]	[***insert relevant details***]
	Elements of Service	**Business requirement**	**HMRC Responsibility**

3.	**Name of Service Recipient:**	**[*Insert name of Service Recipient*]**	
	Service line	**Service Description**	**Charging reference**
	[***insert relevant details***]	[***insert relevant details***]	[***insert relevant details***]
	Elements of Service	**Business requirement**	**HMRC Responsibility**

4.	**Name of Service Recipient:**	**[*Insert name of Service Recipient*]**	
	Service line	**Service Description**	**Charging reference**
	[***insert relevant details***]	[***insert relevant details***]	[***insert relevant details***]

	Elements of Service	Business requirement	HMRC Responsibility

5.	Name of Service Recipient:	[*Insert name of Service Recipient*]	
	Service line	**Service Description**	**Charging reference**
	[*insert relevant details*]	[*insert relevant details*]	[*insert relevant details*]
	Elements of Service	**Business requirement**	**HMRC Responsibility**

2 SERVICE BENEFICIARIES

The table below sets out an indicative and non-exhaustive list

	ExtOrg	DataFlow Title	DataFlow Description	System	Medium	Process	Process Description	Number of Users (where relevant)
1								
2								
3								

HM Revenue & Customs

HMRC Tier 1 and 2 Model ICT Contract
Version 2.3 (December 2020)

SCHEDULE 2.8 | Data Processing and List of Sub-Processors

Schedule 2.8 | Data Processing and List of Sub-Processors

INTRODUCTION

(a) Part A of this Schedule lists the types of Personal Data and categories of Data Subject which the Supplier will Process in its provision of the Services together with a description of the nature, purposes and duration of the Processing, the subject matter of the Processing, and the retention policy in respect of that data, and has been collated in accordance with Clause 23.2(a) and (b).

(b) Part B of this Schedule lists the Sub-Processors agreed by the Parties in accordance with Clause 23.5.

Part A | Data Processing

1. The Supplier shall comply with any further written instructions with respect to Processing by the Authority.

2. Any such further instructions shall be incorporated into this Schedule.

Output Services

Description	Details
Subject matter of the processing	**REDACTED**
Duration of the processing	**REDACTED**
Nature and purposes of the processing	**REDACTED**

Type of personal data	**REDACTED**
Categories of data subjects	**REDACTED**
Plan for return and destruction of the data once the processing is complete UNLESS requirement under UK, EU or member state law to preserve that type of data	**REDACTED**

Input services

Description	**Details**
Subject matter of the processing	**REDACTED**
Duration of the processing	**REDACTED**
Nature and purposes of the processing	**REDACTED**
Type of personal data	**REDACTED**

Categories of data subjects	**REDACTED**
Plan for return and destruction of the data once the processing is complete UNLESS requirement under UK, EU or member state law to preserve that type of data	**REDACTED**

Email & Mobile Messaging Services

Description	**Details**
Subject matter of the processing	**REDACTED**
Duration of the processing	**REDACTED**
Nature and purposes of the processing	**REDACTED**
Type of personal data	**REDACTED**

Categories of data subjects	**REDACTED**
Plan for return and destruction of the data once the processing is complete UNLESS requirement under UK, EU or member state law to preserve that type of data	**REDACTED**

Part B | Sub-Processors as at The Effective Date

[List of Sub-processors to be populated by Supplier within 3 months of Contract Signature]