Department for Work & Pensions

SCHEDULE 2

SERVICE REQUIREMENTS

2.1 Services Description (Specification)

2.2 Tender Minimum Performance Levels and Performance Reviews

2.3 Standards

2.4 Security Requirements

2.5 Insurance Requirements

SCHEDULE 2.1 - SERVICES DESCRIPTION (SPECIFICATION)

Description of the Services

The Supplier will comply with the detail set out within the following additional documents which shall be deemed to be incorporated into this Agreement;

Document	Dated
Specification	V1.0 Final Issued on the E-Procurement System as part of the ITT on 09/10/2020 15:45:17 a copy of which is attached at Annex A to this Schedule 2.1.
Q&A Log (Q&A)	Response to the Q&A Log during the period **15 – 29 October 2020**, as posted on the E-Procurement System on 29/10/2020 08:54:07 a copy of which is attached at Annex B to this Schedule 2.1.

Annex A: Specification

JETS Scotland T&Cs Sch 02 1A - JETS Scot

JETS Scotland T&Cs Sch 02 1A - Deferral c

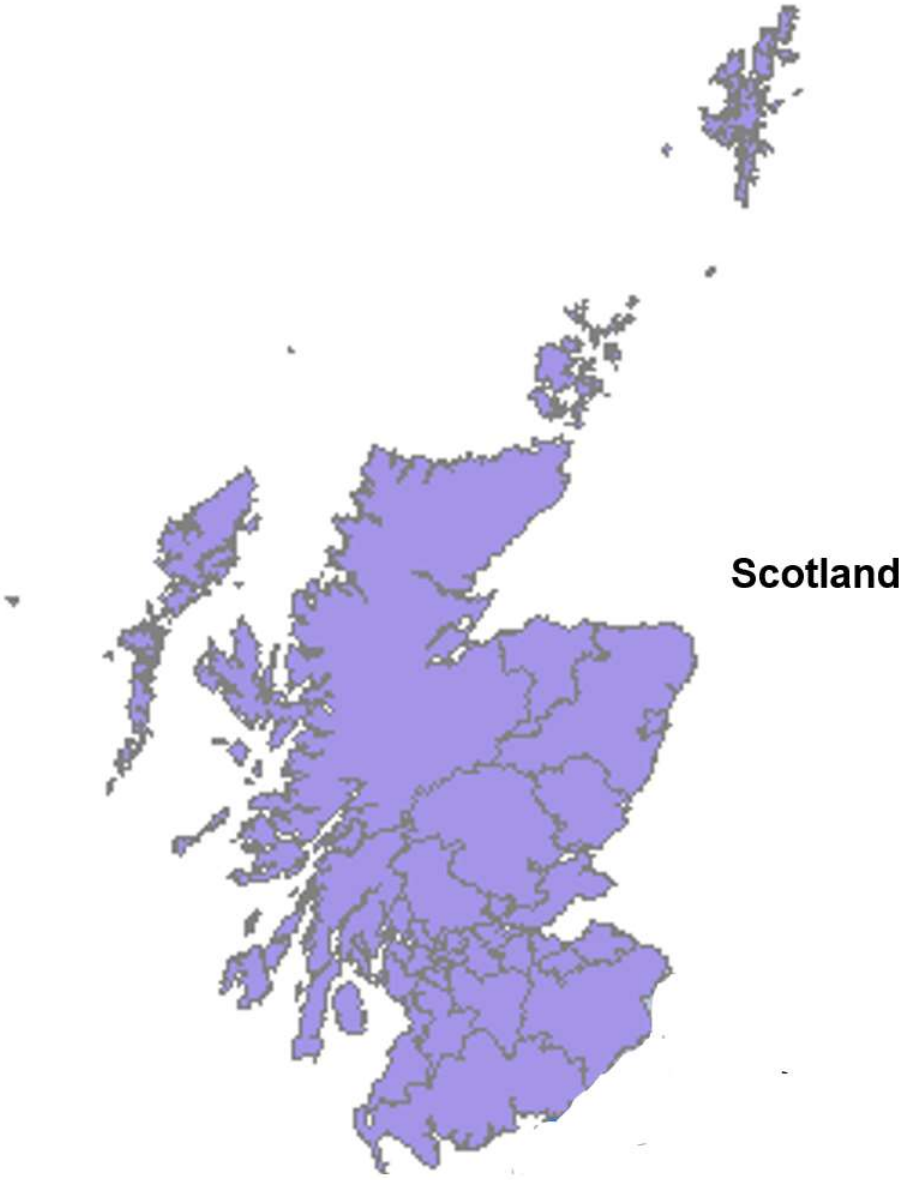
Annex B: Q&A Log

Published Log 6 - Final Log.pdf

Annex C: Contract Package Area

Single CPA Scotland

CONTRACT PACKAGE AREA INFORMATION



1 Local Authorities within Contract Package Area

Scotland
Aberdeen City
Aberdeenshire
Angus
Argyll and Bute
City of Edinburgh
Clackmannanshire
Dumfries and Galloway
Dundee City
East Ayrshire
East Dunbartonshire
East Lothian
East Renfrewshire
Eilean Siar
Falkirk
Fife
Glasgow City
Highland
Inverclyde
Midlothian
Moray
North Ayrshire
North Lanarkshire
Perth and Kinross
Renfrewshire
Scottish Borders
South Ayrshire
South Lanarkshire
Stirling
West Dunbartonshire
West Lothian

SCHEDULE 2.2 –MINIMUM PERFORMANCE LEVELS AND PERFORMANCE REVIEWS

(MPLs and CSSs)

1 Minimum Performance Levels (MPLs)

MPL	1	MPL for the CPA. **Notes**: This is the headline performance target; a CPA-level % conversion rate taken from the tender offers, set at a minimum of 20% will be applied. Performance will be measured and managed on a cohort and cohort profile basis.

1.1 The MPLs are based on a predicted number of Participant Starts.

1.2 Without prejudice to the Authority's right to undertake check(s) pursuant to Clause C4, for performance management purposes only, the Authority may measure the Supplier's performance against each MPL at any time based on the assumption that each Outcome in the period for which the Authority is measuring the Supplier's performance against such MPL would satisfy all of the relevant qualifying criteria and requirements (in respect of that Outcome). For the avoidance of doubt, this includes any Performance Improvement Notice issued by the Authority in relation to a Service Failure pursuant to Clause B5.

2 Customer Service Standards

CSS	1	The Provider must acknowledge 99.5% of Referrals on PRaP within 2 (two) Working Days of receipt of a Referral. This will be monitored through the PRaP system.
	2	No more than 4% of Referrals will be in Backlog at any one time. Backlog means an accumulation of uncompleted work or matters needing to be dealt with in relation to CSS1 or 3. This will be monitored through PRaP
	3	No single Referral will be in Backlog for more than 25 Working Days of receiving the Referral. This will be monitored through PRaP.
	4	The Provider will contact potential JETS Scotland Participants within 2 (two) Working Days of receiving a Referral, to set up an initial appointment between the Provider and the potential JETS Scotland Participant.

	5	The initial appointment will take place within 15 (fifteen) Working Days of the Provider receiving the Referral. The Provider must also update PRaP with: (i) a start, (ii) did not attend or (iii) did not start by the 15th (fifteenth) Working Day for 99% of referrals. This will be monitored through the PRaP system.
	6	The Provider will provide the Participant with a copy of the customer service standards within 1 (one) Working Day of becoming a Participant. The customer service standards referred to here are details on the support that the Provider can provide to the Participant.
	7	The Provider will work with the Participant to explore the Participant's ambitions, goals, priorities and personal needs. This will help formulate an Action Plan. This Action Plan must be finalised within 10 (ten) Working Days of the Participant Start.
	8	The Provider will engage the Participant (by telephone/video conference or any other method permitted by the Contract) every 10 (ten) Working Days as a minimum, to discuss the Participant's wellbeing, Action Plan and job goals ("Booked Meeting"). The frequency of the Booked Meetings can be amended if the Participant prefers a different arrangement
	9	If the Participant misses a Booked Meeting and the Provider is not contacted by the Provider with an explanation as to why, the Provider will attempt to contact the Participant within 2 (two) Working Days with a view to resolving any issues
	10	If the Participant is not in employment or self-employment at the point they cease to be a Participant, the Provider will produce an Exit Report. The Exit

		Report will include a summary of the Participant's time on JETS Scotland, along with details of additional support that can be accessed to support them going forward. The Exit Report will be provided to Participants within the last 10 (ten) Working Days of the Participant being a Participant. The Provider will also maintain a copy of the Exit Report securely, which must be sent to the Contracting Body upon request from the Contracting Body.
	11	Every month, the Provider will be required to obtain information from the Participants on the usefulness of the Programme (see Customer Insight section) The Provider will collate Participant responses in the template to be provided by the Contracting Body. The Provider will send the completed template to the Contracting Body by the 15th day of the following calendar month. If the 15th day happens to be a non-Working Day, then the deadline shall move to the next Working Day.

3 Contract Performance Reviews

3.1 The Authority will conduct regular formal Contract Performance Review meetings ("**CPRs**") at a frequency determined by the Authority from time to time to monitor, measure and review the Supplier's performance, utilising the Authority's Performance Management and Intervention Regime ("**PMIR**"), which is described in the Provider Guidance. CPRs will encourage an open and regular dialogue between the Authority and the Supplier with the purpose of ensuring that the Services are being supplied in accordance with the Minimum Performance Levels (MPLs) and the Customer Service Standards are being achieved. CPRs will be formally conducted and documented.

3.2 The Supplier shall:

(a) co-operate fully with the Authority; and

(b) supply all information requested by the Authority; and

(c) arrange access to Sites requested by the Authority,

for the purposes of conducting the CPRs.

4 Supplier Systems Assurance

4.1 The Supplier shall comply with the Authority's requirements for Supplier Systems Assurance as described in this paragraph 4 of Schedule 2.2 and notified to the Supplier by the Authority from time to time.

4.2 The primary purpose of the Supplier Systems Assurance is to provide the Authority with an assurance that payments to Suppliers are in accordance with the Authority and HM Treasury policies, that public funds are protected and that value for money has been obtained.

4.3 Provider Assurance Team Review(s) ("**PAT Reviews**") will be carried out on the Suppliers' internal control systems to assess the Suppliers' ability to manage risk across three key areas:

a) Governance Arrangements – covering the Supplier's governance arrangements, systems for tracking and reporting performance and their anti-fraud measures;

b) Service Delivery – includes the Supplier's systems for starting, ending and moving Participants through the Services and generally looks to ensure that the Authority is getting the services for which it is paying. This section also covers management of the supply chain; and

c) Claim Procedures and Payments – looks to ensure that Suppliers have in place effective systems to support their claims for payment, including appropriate segregation of duties.

4.4 On completion of each review by the Authority, the Supplier will be awarded an assurance rating in one of the following four categories – (i) weak: (ii) limited; (iii) reasonable; or (iv) strong (each a "**Supplier Assurance Rating**"). The Authority shall also send a formal report to the Supplier which details the PAT Review findings including key strengths and areas for improvement; where weaknesses have been identified the Supplier will be asked to complete an action plan setting out appropriate steps for improvement (a "**PAT Action Plan**") and this is followed up at an agreed point.

4.5 The timescale for a subsequent review is determined at the sole discretion of the Authority.

4.6 If the Supplier is attributed a "Weak" or "Limited" Supplier Assurance Rating, as notified to the Supplier by the Authority from time to time, the Supplier shall deploy all additional resources and take all remedial action that is necessary to remedy the "Weak" or "Limited" Supplier Assurance Rating or to prevent the "Weak" or "Limited" Supplier Assurance Rating from recurring by a date specified by the Authority.

4.7 If in the opinion of the Authority, the Supplier has failed to deploy the required additional resources and to take the remedial action in accordance with the PAT Action Plan by the date specified by the Authority, the Authority may treat such failure as a Non Service Failure Default and issue a Formal Warning Notice in accordance with Clause B15.

4.8 The Authority shall be entitled to terminate the Agreement by issuing a Termination Notice to the Supplier in the following circumstances:

a) where the Supplier has been awarded a Supplier Assurance Rating of "Weak" or "Limited", as notified to the Supplier by the Authority from time to time, in two (2) separate consecutive PAT Reviews for reasons which the Authority regards, at its sole discretion, as similar reasons; or

b) where the Supplier has been awarded a Supplier Assurance Rating of "Weak" or "Limited" as notified to the Supplier by the Authority from time to time, in three (3) separate consecutive PAT Reviews regardless of the reasons for such award; or

c) on-going or repeated failures on the part of the Supplier to comply with and implement a PAT Action Plan.

4.9 Notwithstanding any other term of this Agreement the Supplier hereby gives its consent for the Authority to publish from time to time any of the Supplier's Supplier Assurance Ratings to the general public and to provide the Supplier's Supplier Assurance Ratings to any person as the Authority deems appropriate. The Supplier shall assist and cooperate with the Authority to enable the Authority to publish and provide the Supplier's Supplier Assurance Ratings to any person the Authority deems appropriate in accordance with this paragraph.

4.10 The Authority will from time to time publish the Supplier's Supplier Assurance levels and

will identify the Supplier by name and the Supplier hereby consents to such publication.

4.11 Further information regarding to the PAT Reviews can be found in the Provider Guidance:

Generic guidance for DWP providers - GOV.UK

5 Performance Indicators

5.1 The Authority shall carry out regular Performance Indicator Reviews at a frequency determined by the Authority from time to time to review the Supplier's performance against the Performance Indicators. The Supplier shall co-operate fully with such Performance Indicator Reviews and shall promptly provide the Authority with all Management Information the Authority requires for the purpose of carrying out such Performance Indicator Reviews.

5.2 Where as a result of the Performance Indicator Review the Authority believes that:

a) the Performance Indicators fall below the required standard; or

b) the Authority, acting reasonably, believes that without intervention the Performance Indicators will fall below the required standard,

then, without prejudice to any other right or remedy it may have under this Agreement, the Authority may issue a Performance Indicator Course of Action Notice requiring the Supplier to implement a Performance Indicator Course of Action in accordance with this Schedule 2.2, paragraph 5.

5.3 A Performance Indicator Course of Action Notice given, in accordance with this Schedule 2.2 paragraph 5, to the Supplier by the Authority may include:

a) confirmation as to how the Performance Indicators fall below or are anticipated to fall below the required standard;

b) the actions the Authority in its absolute discretion requires the Supplier to take to satisfy the Authority that the Supplier can ensure compliance with its contractual obligations in relation to Performance Indicators; and

c) the time period during which the Supplier is expected to follow the Performance Indicator Course of Action to achieve improvement of the Performance Indicators.

5.4 For the avoidance of doubt, the Authority may initiate the Performance Indicator Course of Action at any time after a Performance Indicator Review and any delay in exercising its right to initiate the Performance Indicator Course of Action shall not constitute a waiver or cause of diminution of the Authority's right to do so.

5.5 For the avoidance of doubt, the Authority shall be under no obligation to initiate the Performance Indicator Course of Action and it may choose in its absolute discretion to exercise any other right or remedy available to it under this Agreement instead of or running in parallel with such right.

5.6 The Supplier shall have the right to respond in relation to the Performance Indicator Course of Action within ten (10) Working Days following notification under paragraph 5.2 and either confirm its acceptance or following discussions with the Authority submit its revised plan. If such revised plan is agreed by the Authority, it shall be the revised Performance Indicator Course of Action.

5.7 Once agreed the Supplier shall immediately implement the Performance Indicator Course of Action. For the avoidance of doubt, any agreement between the Parties in relation to the Performance Indicator Course of Action shall not relieve the Supplier of any of its

liabilities and obligations under this Agreement.

5.8 If a revised Performance Indicator Course of Action cannot be agreed within the period of ten (10) Working Days (or such other period as notified by the Authority to the Supplier) then the Authority may elect to refer the matter for resolution by the Dispute Resolution Procedure set out in Clause J11.

5.9 Performance Indicators

PERFORMANCE INDICATORS

This is the % conversion rate taken from the tender offer, set at 20%. Performance will be measured and managed on a cohort basis and against the agreed Performance Curve included in the tender.

SCHEDULE 2.3 - STANDARDS

Standards

2 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.

3 General

3.1 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.

3.2 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 (in a reasonable timeframe), prior to the implementation of the new or emergent standard.

3.3 Where Standards referenced conflict with each other or with Good Industry Practice, then the later Standard or best practice shall be adopted by the Supplier. Any such alteration to any Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

4 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.

5 Open data standards & Standards Hub

5.1 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.

5.2 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.

5.3 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.

6 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 TOGAF 9.1 or its equivalent, then this shall be deemed acceptable.

7 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) 2.0 Conformance Level AA; and

(b) ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability.

8 Service management software & standards

8.1 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 v3 2011;

(b) ISO/IEC 20000-1 2011 "ITSM Specification for Service Management";

(c) ISO/IEC 20000-2 2012 "ITSM Code of Practice for Service Management";

(d) ISO 10007 "Quality management systems – Guidelines for configuration management"; and

(e) BS25999-1:2006 "Code of Practice for Business Continuity Management" and, ISO/IEC 27031:2011, ISO 22301 and ISO/IEC 24762:2008 in the provision of "IT Service Continuity Strategy" or "Disaster Recovery" plans.

8.2 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.

9 Environmental standards

9.1 The Supplier warrants that it has obtained ISO 14001 (or equivalent) certification for its environmental management and shall comply with and maintain certification requirements throughout the Term. The Supplier shall follow a sound environmental management policy, ensuring that any Goods and the Services are procured, produced, packaged, delivered, and are capable of being used and ultimately disposed of in ways appropriate to such standard.

9.2 The Supplier shall comply with relevant obligations under the Waste Electrical and

Electronic Equipment Regulations 2006 in compliance with Directive 2002/96/EC and subsequent replacements (including those in compliance with Directive 2012/19/EU).

9.3 The Supplier shall (when designing, procuring, implementing and delivering the Services) ensure compliance with Article 6 and Annex III of the Energy Efficiency Directive 2012/27/EU and subsequent replacements.

9.4 The Supplier shall comply with the EU Code of Conduct on Data Centres' Energy Efficiency. The Supplier shall ensure that any data centre used in delivering the Services are registered as a Participant under such Code of Conduct.

9.5 The Supplier shall comply with the Authority and HM Government's objectives to reduce waste and meet the aims of the Greening Government: IT strategy contained in the document "Greening Government: ICT Strategy issue (March 2011)" at https://www.gov.uk/government/publications/greening-government-ict-strategy.

10 Hardware safety standards

10.1 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 60950-1:2006+A12:2011 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 60065:2002+A12:2011 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 60825-1:2007 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 41003:2009 or any subsequent replacements.

10.2 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.

SCHEDULE 2.4 - SECURITY REQUIREMENTS TIER 1 AND 2

General

The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Authority's security requirements as set out in the Agreement which include the requirements set out in this Schedule 2.4 to the Agreement (the "**Authority's Security Requirements**"). The Authority's Security Requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Authority Assets, the Authority System and the Supplier System.

Terms used in this Schedule 2.4 which are not defined below shall have the meanings given to them in Schedule 1 (Definitions) of the Agreement.

1. Definitions

1.1 In this Schedule 2.4, the following definitions shall apply:

"**Authority Personnel**"	shall mean all persons employed by the Authority including directors, officers, employees together with the Authority's servants, agents, consultants, contractors and suppliers but excluding the Supplier and any Sub-contractor (as applicable).
"**Availability Test**"	shall mean the activities performed by the Supplier to confirm the availability of any or all components of any relevant ICT system as specified by the Authority.
"**CHECK**"	shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.
"**Cloud**"	shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data.
"**Cyber Essentials Plus**"	shall mean the Government-backed, industry-supported scheme managed by the NCSC with higher level of security requirements to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
"**Cyber Security Information Sharing Partnership**" or "**CiSP**"	shall mean the cyber security information sharing partnership established by the NCSC or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
"**Good Security Practice**"	shall mean: a) the technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for Standardization or the National Institute of Standards and Technology); b) security standards and guidelines relating to Information

Security (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) provided to the general public or Information Security practitioners and stakeholders by generally recognised authorities and organisations; and

c) the Government's security policies, frameworks, standards and guidelines relating to Information Security.

"Information Security" shall mean:

a) the protection and preservation of:

i) the confidentiality, integrity and availability of any Authority Assets, the Authority System (or any part thereof) and the Supplier System (or any part thereof);

ii) related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and

b) compliance with all Law applicable to the processing, transmission, storage and disposal of Authority Assets.

"Information Security Manager" shall mean the person appointed by the Supplier with the appropriate experience, authority and expertise to ensure that the Supplier complies with the Authority's Security Requirements.

"Information Security Management System ("ISMS")" shall mean the set of policies, processes and systems designed, implemented and maintained by the Supplier to manage Information Security Risk as certified by ISO/IEC 27001.

"Information Security Questionnaire" shall mean the Authority's set of questions used to audit and on an ongoing basis assure the Supplier's compliance with the Authority's Security Requirements.

"Information Security Risk" shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.

"ISAE 3402" shall mean the International Standard on Assurance Engagements No. 3402 (ISAE) as most recently published by the International Auditing and Assurance Standards Board or its successor entity ("**IAASB**") or the relevant successor or replacement standard which is formally recommended by the IAASB.

"ISO/IEC 27001, ISO/IEC 27002 and ISO 22301 shall mean:

a) ISO/IEC 27001;

b) ISO/IEC 27002/IEC; and

c) ISO 22301

in each case as most recently published by the International Organization for Standardization or its successor entity (the "**ISO**") or the relevant successor or replacement information security standard which is formally recommended by the ISO.

"**NCSC**"	shall mean the National Cyber Security Centre or its successor entity (where applicable).
"**Penetration Test**"	shall mean a simulated attack on any Authority Assets, the Authority System (or any part thereof) or the Supplier System (or any part thereof).
"**PCI DSS**"	shall mean the Payment Card Industry Data Security Standard as most recently published by the PCI Security Standards Council, LLC or its successor entity (the "**PCI**").
"**Risk Profile**"	shall mean a description of any set of risks. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable.
"**Security Test"**	shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.
"**SSAE 16**"	shall mean the Statement on Standards for Attestation Engagements (SSAE) No. 16 as most recently published by the American Institute of Certified Public Accountants or its successor entity ("**AICPA**") or the relevant successor or replacement standard which is formally recommended by the AICPA.
"**Tigerscheme**"	shall mean a scheme for authorised penetration tests which scheme is managed by USW Commercial Services Ltd.
"**Vulnerability Scan**"	shall mean an ongoing activity to identify any potential vulnerability in any Authority Assets, the Authority System (or any part thereof) or the Supplier System (or any part thereof).

1.2 Reference to any notice to be provided by the Supplier to the Authority shall be construed as a notice to be provided by the Supplier to the Authority Representative.

2 Principles of security

2.1 The Supplier shall at all times comply with the Authority's Security Requirements and provide a level of security which is in accordance with the Security Policies and Standards, Good Security Practice and Law.

3 ISO/IEC 27001 compliance, certification and Audit

3.1 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, obtain and maintain certification to ISO/IEC 27001 (the "**ISO Certificate**") in relation to the Services during the Term. The ISO Certificate shall be provided by the Supplier to the Authority on the dates as agreed by the Parties.

3.2 The Supplier shall appoint:

a) an Information Security Manager; and

b) a deputy Information Security Manager who shall have the appropriate experience, authority and expertise to deputise for the Information Security Manager when s/he is on leave or unavailable for any period of time.

The Supplier shall notify the Authority of the identity of the Information Security Manager on the Effective Date and, where applicable, within five (5) Working Days following any change in the identity of the Information Security Manager.

3.3 The Supplier shall ensure that it operates and maintains the Information Security Management System during the Term and that the Information Security Management System meets the Security Policies and Standards, Good Security Practice and Law and includes:

a) a scope statement (which covers all of the Services provided under this Agreement);

b) a risk assessment (which shall include any risks specific to the Services);

c) a statement of applicability;

d) a risk treatment plan; and

e) an incident management plan

in each case as specified by ISO/IEC 27001.

The Supplier shall provide the Information Security Management System to the Authority upon request within ten (10) Working Days from such request.

3.4 The Supplier shall notify the Authority of any failure to obtain an ISO Certificate or a revocation of an ISO Certificate within two (2) Working Days of confirmation of such failure or revocation. The Supplier shall, at its own expense, undertake those actions required in order to obtain an ISO Certificate following such failure or revocation and provide such ISO Certificate within one calendar month of the initial notification of failure or revocation to the Authority or on a date agreed by the Parties.

3.5 The Supplier shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within ten (10) Working Days after completion of the relevant audit provide any associated security audit reports to the Authority.

3.6 Notwithstanding the provisions of paragraph 3.1 to paragraph 3.5, the Authority may, in its absolute discretion, notify the Supplier that it is not in compliance with the Authority's Security Requirements and provide details of such non-compliance. The Supplier shall, at its own expense, undertake those actions required in order to comply with the Authority's Security Requirements within one calendar month following such notification or on a date as agreed by the Parties.

4 Cyber Essentials Plus scheme

4.1 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, obtain and maintain certification to Cyber Essentials Plus (the "Cyber Essentials Plus Certificate") in relation to the Services during the Term. The Cyber Essentials Plus Certificate shall be provided by the Supplier to the Authority annually on the dates as agreed by the Parties.

4.2 The Supplier shall notify the Authority of any failure to obtain, or the revocation of, a Cyber Essentials Plus Certificate within two (2) Working Days of confirmation of such failure or revocation. The Supplier shall, at its own expense, undertake those actions required in order to obtain a Cyber Essentials Plus Certificate following such failure or revocation.

5 Risk Management

5.1 The Supplier shall operate and maintain policies and processes for risk management (the **Risk Management Policy**) during the Term which includes standards and processes for the assessment of any potential risks in relation to the Services and processes to ensure that the Authority's Security Requirements are met (the **Risk Assessment**). The Supplier shall provide the Risk Management Policy to the Authority upon request within ten (10) Working Days of such request. The Authority may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Authority's Security Requirements. The Supplier shall, at its own expense, undertake those actions required in order to implement the changes required by the Authority within one calendar month of such request or on a date as agreed by the Parties.

5.2 The Supplier shall carry out a Risk Assessment:

(i) at least annually;

(ii) in the event of a material change in the Supplier System or in the threat landscape; or

(iii) at the request of the Authority.

The Supplier shall provide the report of the Risk Assessment to the Authority, in the case of at least annual Risk Assessments, within five (5) Working Days of completion of the Risk Assessment or, in the case of all other Risk Assessments, within one calendar month after completion of the Risk Assessment or on a date as agreed by the Parties. The Supplier shall notify the Authority within five (5) Working Days if the Risk Profile in relation to the Services has changed materially, for example, but not limited to, from one risk rating to another risk rating.

5.3 If the Authority decides, at its absolute discretion, that any Risk Assessment does not meet the Authority's Security Requirements, the Supplier shall repeat the Risk Assessment within one calendar month of such request or as agreed by the Parties.

5.4 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, co-operate with the Authority in relation to the Authority's own risk management processes regarding the Services.

5.5 For the avoidance of doubt, the Supplier shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this paragraph 5.

6 Security Audit and Assurance

6.1 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, complete the information security questionnaire in the format stipulated by the Authority (the "**Information Security Questionnaire**") at least annually or at the request by the Authority. The Supplier shall provide the completed Information Security Questionnaire to the Authority within one calendar month from the date of request.

6.2 The Supplier shall conduct Security Tests to assess the Information Security of the Supplier System and, if requested, the Authority System. In relation to such Security Tests, the Supplier shall appoint a third party which:

i) in respect of any Penetration Test, is duly accredited by CHECK, CREST (International), or Tigerscheme; and

ii) in respect of any Security Test to which PCI DSS apply, is an approved scanning vendor duly accredited by the PCI.

Such Security Test shall be carried out:

i) at least annually;

ii) in the event of a material change in the Supplier System or in the Authority System; or

iii) at the request of the Authority which request may include, but is not limited to, a repeat of a previous Security Test.

The content, and format of any report of such Security Tests shall be approved in advance of the Security Test by the Authority. The Supplier shall provide any report of such Security Tests within one calendar month following the completion of such Security Test or on a date agreed by the Parties. The Supplier shall, at its own expense, undertake those actions required to rectify any risks identified by any Security Test in the manner and within the timeframe required by the Authority in its absolute discretion.

6.3 The Authority shall be entitled to send the Authority Representative to witness the conduct of any Security Test. The Supplier shall provide to the Authority notice of any Security Test at least one month prior to the relevant Security Test.

6.4 Where the Supplier provides code development services to the Authority, the Supplier shall comply with the Authority's Security Requirements in respect of code development within the Supplier System and the Authority System.

6.5 Where the Supplier provides software development services, the Supplier shall comply with the code development practices specified in the Specification or in the Authority's Security Requirements.

6.6 The Authority, or an agent appointed by it, may undertake Security Tests in respect of the Supplier System after providing advance notice to the Supplier. If any Security Test identifies any non-compliance with the Authority's Security Requirements, the Supplier shall, at its own expense, undertake those actions required in order to rectify such identified non-compliance in the manner and timeframe as stipulated by the Authority at its absolute discretion. The Supplier shall provide all such co-operation and assistance in relation to any Security Test conducted by the Authority as the Authority may reasonably require.

6.7 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, engage an independent auditor registered with the AICPA or, as the case may be, the IAASB (such auditors, the "**SOC Auditors**") to conduct a service organisation control ("**SOC**") 1 Type 2 audit ("**SOC1T2**") and a SOC2 Type 2 audit ("**SOC2T2**") in accordance with the SSAE 16 and/or ISAE 3402.

6.8 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, maintain at least annual renewals of SOC1T2 and SOC2T2 in accordance with SSAE 16 and/or ISAE 3402 during the Term and provide the Authority with a copy of the applicable SOC1T2 report and SOC2T2 report on the dates as agreed by the Parties.

6.9 The Supplier shall agree in advance with the Authority the trust services criteria which shall apply to SOC1T2 and SOC2T2 (the "TSC") in respect of security, confidentiality, integrity, availability and privacy (each as defined by the TSC published by the AICPA or, as the case may be, the IAASB). The Supplier shall provide the SOC1T2 report and SOC2T2 report to the Authority within ten (10) Working Days after receipt from its SOC Auditors.

6.10 In addition to the provisions set out in paragraphs 6.1 to 6.9, the Supplier shall provide a bridge letter in relation to SOC1T2 and SOC2T2 at the reasonable request of the

Authority. The content and format of such bridge letter shall be approved by the Authority in advance and shall be provided within one calendar month of the Authority's request.

6.11 The Authority shall schedule regular security governance review meetings which the Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, attend.

7 PCI DSS compliance and certification

7.1 Where the Supplier obtains, stores, processes or transmits payment card data, the Supplier shall comply with the PCI DSS.

7.2 The Supplier shall obtain and maintain up-to-date attestation of compliance certificates ("**AoC**") provided by a qualified security assessor accredited by the PCI and up-to-date reports on compliance ("**RoC**") provided by a qualified security assessor or an internal security assessor, in each case accredited by the PCI (each with the content and format as stipulated by the PCI and such reports the "PCI Reports"), during the Term. The Supplier shall provide the respective PCI Reports to the Authority upon request within ten (10) Working Days of such request.

7.3 The Supplier shall notify the Authority of any failure to obtain a PCI Report or a revocation of a PCI Report within two (2) Working Days of confirmation of such failure or revocation. The Supplier shall, at its own expense, undertake those actions required in order to obtain a PCI Report following such failure or revocation within one calendar month of such failure or revocation.

8 Security policies and standards

8.1 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Security Policies and Standards set out in Annex A and B.

8.2 Notwithstanding the foregoing, the Authority's Security Requirements applicable to the Services may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the Services. Where any such change constitutes a Change to the Agreement, any change in the Authority's Security Requirements resulting from Change (if any) shall be agreed by the Parties in accordance with the Change Control Procedure. Where any such change constitutes an Operational Change, any change in the Authority's Security Requirements resulting from such Operational Change (if any) shall be implemented in accordance with the paragraphs in Schedule 8.2 (Change Control Procedure) concerning Operational Changes.

8.3 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Standards.

9 Cyber Security Information Sharing Partnership

9.1 The Supplier shall be a member of the Cyber Security Information Sharing Partnership during the Term. The Supplier shall participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.

9.2 The Supplier shall review the NCSC weekly threat reports on a weekly basis and implement recommendations in line with the Supplier's Risk Management Policy.

ANNEX A – AUTHORITY SECURITY POLICIES

The Security Policies are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards unless specified otherwise:

a) Policy: Acceptable Use

b) Policy: Information Security

c) Policy: Physical Security

d) Policy: Information Management

e) Policy: Email

f) Policy: Technical Vulnerability Management

g) Policy: Remote Working Security

h) Policy: Social Media

i) Policy: Data Sharing

j) Policy: Forensic Readiness

k) Policy: SMS Texting

l) Policy: Privileged Users Security

m) Policy: User Access Control

n) Policy: Security Classification

o) Policy: Cryptographic Key Management

p) Policy :NSC Secure Sanitisation of Storage Media (published on https;//www.nsc-gov.uk/guidance/secure sanitisation storage-media

[**Policies highlighted in yellow have not been published yet**]

q) HMG Personnel Security Controls – May 2018

(published on https://www.gov.uk/government/publications/hmg-personnel-security-controls)

ANNEX B – SECURITY STANDARDS

The Security Standards are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards:

a) Security standard SS-001 (part 1): Access and Authentication Controls

b) Security standard SS-001 (part 2): Privileged User Access Controls

c) Security standard SS-002: Public Key Infrastructure & Key Management

d) Security standard SS-003: Software Development

e) Security standard SS-005: Database Management System

f) Security standard SS-006: Security Boundaries

g) Security standard SS-007: Use of Cryptography

h) Security standard SS-008: Server Operating System

i) Security standard SS-009: Hypervisor

j) Security standard SS-010: Desktop Operating System

k) Security standard SS-011: Containerisation

l) Security standard SS-012: Protective Monitoring Standard

m) Security standard SS-013: Firewall Security

n) Security standard SS-014: Security Incident Management

o) Security standard SS-015: Malware Protection

p) Security standard SS-016: Remote Access

q) Security standard SS-017: Mobile Device

r) Security standard SS-018: Network Security Design

s) Security standard SS-019: Wireless Network

t) Security standard SS-022: Voice & Video Communications

u) Security standard SS-023: Cloud Computing

v) Security standard SS-025: Virtualisation

w) Security standard SS-028: Microservices Architecture

x) Security standard SS-029: Securely Serving Web Content

y) Security Standard SS-030: Oracle Database Security

z) Security Standard SS-031: Domain Management

aa) Security Standard SS-033: Security Patching

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;

(c) regulated by the applicable regulatory body and is in good standing with that regulator; and

(d) except in the case of any Insurances provided by an Affiliate of the Supplier, of good repute in the international insurance market.

1.4 The Supplier shall ensure that the public and products liability policy shall contain an indemnity to principals 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 Cancellation

5.1 Subject to Paragraph 5.2, 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.

5.2 Without prejudice to the Supplier's obligations under Paragraph 4, Paragraph 5.1 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.

6 Insurance claims, premiums and deductibles

6.1 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.

6.2 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.

6.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

6.4 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 **£10,000** 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 physical 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 respect of any one occurrence, the number of occurrences being unlimited in any annual policy period, but *100% (one hundred per cent) of the total annual contract value* 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

6.1 Indemnity to principals 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 arising out of 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.

Maximum deductible threshold

Not to exceed [REDACTED] for each and every third party property damage claim (personal injury claims to be paid in full).

Part C: United Kingdom compulsory insurances

The Supplier shall meet its insurance obligations under applicable Law in full, including, United Kingdom employers' liability insurance and motor third party liability insurance.

Part D: 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 specific 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 the limits of the indemnity under the insurance policy that the Insured has in place as at the Effective Date in respect of any one claim and in the aggregate per annum, exclusive of defence costs which are payable in addition.

4 Territorial limits

As in the insurance policy that Insured has in place as at the Effective Date.

5 Period of insurance

From the Effective Date 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 the applicable maximum deductible threshold in the insurance policy that Insured has in place as at the Effective Date for each and every claim.