CONTRACT

For

Service Transformation Support Services

Between

THE SECRETARY OF STATE FOR WORK AND PENSIONS
(the "Authority") acting as part of the Crown

And

The Management Consulting Bureau Limited
(NI673952)

CONTRACT REFERENCE NUMBER: 24943

CONTENTS

This Contract is made on the 13th April 2022

between the Parties

The Secretary of State for Work and Pensions ("**the Authority**") acting as part of the Crown, of Caxton House, Tothill Street, London, SW1H 9DA.

And

The Management Consulting Bureau Limited, with Number Company Registration NI673952, having the main or registered office at 34 Ward Avenue, Bangor, Northern Ireland, BT20 5HP ("**the Contractor")**

individually referred to as **"Party"** and collectively as **"the Parties"**.

FORM OF AGREEMENT

This Contract has been entered into on the Commencement Date stated at A2 – Initial Contract Period.

SIGNED for and on behalf of The Secretary of State for Work and Pensions (**the Authority**)	**SIGNED** for and on behalf of The Management Consulting Bureau Limited (**the Contractor**)
Name: [REDACTED]	**Name: [REDACTED]**
Position: [REDACTED]	**Position:** Company Director
Signature: [REDACTED]	**Signature: [REDACTED]**

TERMS & CONDITIONS

Terms_Conditions%
20final.docx

SCHEDULE 1 THE SERVICES

1 General

The Authority considers the supply under this Contract to be a fully contracted-out service and as such, the Contractor is deemed to be the end client for the purpose of the off-payroll working legislation and are responsible for assessing whether the legislation applies.

This Call-Off Contract is for the Services, with outcome based deliverables detailed in the table below and will be operated as follows:

- The Supplier Staff will be under the day to day direction and control of the Supplier, not DWP;
- Any quality and non-delivery issues will be raised by DWP directly with the Supplier rather than the individual Supplier Staff;
- The Supplier will be held accountable by DWP for non-delivery of the Services, not the individual Supplier Staff;
- The Supplier is able to substitute the individual Supplier Staff to undertake the Services within this Call-Off Contract as long as they have the equivalent experience and qualifications of the substituted individual Supplier Staff member;
- This contract will not be used to fill roles that already exist in DWP.

The Supplier will deliver the following outcome based deliverables (the “Services”)

1. WORKSHOP PREP – including interviews with team members & create workshop material (2 weeks)

2. OFFSITE WORKSHOP, OUTPUTS AND RECOMMENDATIONS – including workshop facilitation and write up (1 week)

Deliverables		**Description**	**Milestones**	**Acceptance Criteria**
1	Workshop Interviews & Preparation	Interviews with 10 team members to document and categorise issues and shape themes to be addressed in the workshop	**End of week 1:** Interview summary of attendees and resulting themes **End of week 2:** Updated interview summary and themes, plus outline agenda for workshop	A PowerPoint document will be issued prior to the workshop

2	Facilitated Off-Site Workshop	Offsite workshop held with senior leaders from DWP	**End of week 3:** Initial roundup of workshop discussions and outcomes refined in final report	A facilitated workshop delivered

SCHEDULE 2 ADMINISTRATION REQUIREMENTS

1 Authority's Authorisation

1.1 The following person is the Authority's Representative and is authorised to act on behalf of the Secretary of State for Work and Pensions on all matters relating to the Contract ("**Authority's Representative**"**)**. Contact details are shown in clause A5.3.

Name: [REDACTED]
Title: Chief Digital & Information Officer

1.2 The Authority's Representative may approve deputy Authority's Representatives to exercise on his/her behalf such powers as are contained in this Contract.

2 Contractor's Authorisation

2.1 The following person is the Contractor's representative and is authorised to act on behalf of the Contractor on all matters relating to the Contract (**"Contractor's Representative"**). Contact details are shown in clause A5.3.

Name: [REDACTED]
Title: Director

3 Payment Information

3.1 The Authority and the Contractor shall exchange all orders, invoices, claims and payments via electronic methods.

3.2 The following information is required to be completed independently from the Contractor before a claim is submitted for payment by the Authority.

a) Milestone Achievement Certificate signed by the Authority Representative confirming milestones have been delivered in accordance with agreed Acceptance Criteria using the attached format.

Milstone%20Achievement%20Certificate.dc

Invoices shall include a valid Purchase Order number which will be provided by the Authority and shall be sent to:

APinvoices-DWP-U@gov.sscl.com.

A copy of the invoice will be emailed to:
[REDACTED] and [REDACTED]

4 Disputed Claims

4.1 Notwithstanding paragraph 4.5 of this Schedule 2, payment by the Authority of all or any part of any Contract Price rendered or other claim for payment by the Contractor shall not signify Approval. The Authority reserves the right to verify Contract Price after the date of payment and subsequently to recover any sums which have been overpaid.

4.2 If any part of a claim rendered by the Contractor is disputed or subject to question by the Authority either before or after payment then the Authority may call for the Contractor to provide such further documentary and oral evidence as it may reasonably require to verify its liability to pay the amount which is disputed or subject to question and the Contractor shall promptly provide such evidence in a form satisfactory to the Authority.

4.3 If any part of a claim rendered by the Contractor is disputed or subject to question by the Authority, the Authority shall not withhold payment of undisputed sums of such claim.

4.4 If any fee rendered by the Contractor is paid but any part of it is disputed or subject to question by the Authority and such part is subsequently agreed or determined not to have been properly payable then the Contractor shall forthwith repay such part to the Authority.

4.5 The Authority shall be entitled to deduct from sums due to the Contractor by way of set-off any amounts owed to it or which are in dispute or subject to question either in respect of the fee for which payment is being made or any previous fee.

5 Final Claims

5.1 Provided all previous claims have been paid, the Authority shall have no further liability to make payment of any kind to the Contractor once the final claims have been paid.

SCHEDULE 3 MONITORING REQUIREMENTS

This Schedule 3 sets out the Contract management requirements which are applicable to the delivery of the Services.

1 Reviewing Contract Performance

1.1 The Contractor shall work with the Authority to establish and maintain an effective and beneficial working relationship to ensure the Contract is delivered as specified.

1.2 The Contractor shall work with the Authority to establish suitable administrative arrangements for the effective management and performance monitoring of the Contract and shall provide information as requested to monitor and evaluate the success of the Contract and the Contractor's management and delivery of it.

1.3 The Contractor shall supply information requested relevant to the delivery of the Services to the Authority, using formats and to timescales specified by the Authority in this Schedule 3.

1.4 The Authority intends, wherever it can, to capture and collate information through its Authority's Systems Environment. However, the Authority does reserve the right to make reasonable requests for information (at no additional charge) from the Contractor including ad-hoc requests for information from time to time.

1.5 Any additional requests for information shall be considered in consultation with the Contractor as shall the process of defining the methods of collection.

1.6 Where an ongoing, short-term or one-off requirement is agreed, both Parties agree that it shall be included, or deemed to be included within this Schedule 3.

1.7 Review meetings between the Authority and the Contractor shall also cover, as appropriate, dispute resolution and/or dealing with contractual breaches in accordance with the terms and conditions of this Contract. Roles and responsibilities will be documented and the personnel involved in managing the relationship identified and suitably empowered.

1.8 The Authority may undertake spot checks at any time to ensure that the Contractor is complying with its obligations under this Contract and the Contractor shall co-operate fully, at its own cost, with the Authority.

1.9 The Contractor will be responsible for managing and reporting on any subcontractual arrangements. Arrangements shall include mechanisms for the provision of management information, including feedback to and from customers and stakeholders; change control procedures and the prompt resolution of any problems. The Authority will agree with the Contractor day-to-day relationship management, contact points, communication flows and escalation procedures.

1.10 The Contractor will be expected to continuously improve the quality of the provision including that delivered by its Sub-contractors. Where quality falls below

acceptable levels (see 1.1 - minimum standard) the Contractor will be expected to have suitable escalation procedures in place to resolve this issue
and, in respect of sub-contracted provision, take action where necessary to terminate the Sub-contract.

2 Access

2.1 In all instances, the Contractor shall co-operate and provide such reasonable assistance as may be necessary to facilitate such monitoring in relation to the Contract. Failure to provide such reasonable assistance shall be deemed a "Default" for the purposes of clause H2 (Termination on Default).

3 Health and Safety Responsibilities of the Authority's Representatives

3.1 The Authority's Representatives may visit Contractors and its Sub-contractors for a variety of reasons. In the course of their normal duties such representatives of the Authority may make recommendations in relation to the monitoring of health and safety requirements. In doing this the Authority's Representatives shall not be conducting a health and safety inspection, nor shall they be in a position to offer advice on whether something is safe or not, which shall remain the responsibility of the Contractor. Instead, they shall approach this from the position of any lay person. If, however, the Authority's Representative does notice something on which they require assurance or clarification, they shall raise this with the Contractor or the Sub-contractor's representative at the location where they are visiting. In no event are the Authority's Representatives to be seen as offering professional advice on health and safety matters and as such, shall not be liable for any advice or comments or otherwise given to the Contractor or its Sub-contractors or any omission to give such advice, comments or otherwise.

4 Management Information

4.1 The Contractor shall supply information relevant to the delivery of the Services upon reasonable request from the Authority.

Management Charges and Information

4.2 In addition to any other management information requirements set out in this Contract, the Contractor agrees and acknowledges that it shall, at no charge to the Authority, provide timely, full, accurate and complete management information reports for SME's to the Authority which incorporate the following data:-

a) the total contract revenue received directly on the contract;

b) the total value of sub-contracted revenues under the contract (including revenues for non-SMEs/non-VCSEs); and

c) the total value of sub-contracted revenues to SMEs and VCSEs.

Appendix A Contract Performance Targets

Key Performance Indicators

1. In delivering the Services the Contractor acknowledges that it is under an obligation to meet the following Key Performance Indicators and furthermore that failure to meet all or any of the specified Key Performance Indicators, shall entitle the Authority to exercise its rights under clause F5.

2. The following Key Performance Indicators shall apply to this Contract:-

Key Performance Indicators
a) Deliverables provided in accordance with specified timescales
b) Deliverables provided to an acceptable standard and quality in line with acceptance criteria outlined

Appendix B Performance Review Table for Contract Management

1. The following definitions shall be used to determine the standard **Performance Rating** in the Contractor's Performance Review Table: -

4	High Standard	Sometimes exceed and consistently achieves the required standard Very few weaknesses Limited management support needed.
3	Acceptable Standard	Meets required standard Few weaknesses Some management support needed
2	Below Standard	Usually meets, but sometimes fails to meet required standard Some weaknesses Considerable management support needed
1	Failure	Cannot meet required standard without excessive management support Many weaknesses

2. Contractor's Performance Review Table:-

Date of Review		
Description	*Score*	*Remarks*
Total		
Comments		
Signed for the Authority	*Date*	
Signed for the Contractor	*Date*	

SCHEDULE 4 – Contract Price

1. A single milestone charge of £50,000 (excluding VAT) shall be payable upon completion and acceptance of the deliverables detailed in Schedule 1 (Services).

2. Expenses shall be paid in line with the Authority's own Travel & Subsistence policy (attached) up to a maximum of £4,000.

DWP%20Travel%20
Policy%20-%20upda

SCHEDULE 5 – COMMERCIALLY SENSITIVE INFORMATION

1. The Authority acknowledges that the Contractor has requested that the following information be treated as Commercially Sensitive Information;

Document	Page Number	Section	Condition or Paragraph Number	Explanation of harm which may result from disclosure and time period applicable to sensitivity.

2. The Contractor acknowledges that circumstances may arise that require disclosure and are outside the control of the Authority, for example, due to a legal requirement including a court order.

3. The Authority will consult with the Contractor on any request for information, identified as Commercially Sensitive, under the FOIA.

4. The Authority reserves the right to disclose any Commercially Sensitive Information held within this Contract in response to a request under the FOIA as set out at clause E5 of this Contract.

5. The Authority will publish without prior consent from the Contractor all information provided by the Contractor **not** identified in this Schedule 5 as constituting Commercially Sensitive Information under the Authority's transparency reporting requirements provided that such disclosure satisfies the requirements of the FOIA.

6. The Authority reserves the right to determine whether any information provided in this Schedule 5 does constitute Commercially Sensitive Information prior to publication.

SCHEDULE 6 – SECURITY REQUIREMENTS LEVEL 1 AND 2

GENERAL

The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Authority's security requirements as set out in the Contract which include the requirements set out in this Schedule 6 to the Contract (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's Systems Environment and the Contractor's Systems Environment.

Terms used in this Schedule 6 which are not defined below shall have the meanings given to them in clause A1 (Definitions and Interpretations) of the Contract.

1. DEFINITIONS

1.1 In this Schedule 6, 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 Contractor and any Sub-contractor (as applicable).
"**Availability Test**"	shall mean the activities performed by the Contractor 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**	shall mean the Government-backed, industry**Plus**" 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 Partnership**" or "**CiSP**"	shall mean the cyber security information **Information Sharing** 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 Organizaion 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's Systems Environment (or any part thereof) and the Contractor's Systems Environment (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 Contractor with the appropriate experience, authority and expertise to ensure that the Contractor 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 Contractor 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 Contractor'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, 27002 and ISO 22301**	shall mean: **ISO/IEC** 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's Systems Environment (or any part thereof) or the Contractor's Systems Environment (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's Systems Environment (or any part thereof) or the Contractor's Systems Environment (or any part thereof).

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

2. PRINCIPLES OF SECURITY

2.1 The Contractor 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 Contractor 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 Contract Period. The ISO Certificate shall be provided by the Contractor to the Authority on the dates as agreed by the Parties.

3.2 The Contractor 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 Contractor shall notify the Authority of the identity of the Information Security Manager on the Commencement Date and, where applicable, within 5 Working Days following any change in the identity of the Information Security Manager.

3.3 The Contractor shall ensure that it operates and maintains the Information Security Management System during the Contract Period 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 Contract);

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 Contractor shall provide the Information Security Management System to the Authority upon request within 10 Working Days from such request.

3.4 The Contractor shall notify the Authority of any failure to obtain an ISO Certificate or a revocation of an ISO Certificate within 2 Working Days of confirmation of such failure or revocation. The Contractor 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. For the avoidance of doubt, any failure to obtain and/or maintain an ISO Certificate during the Contract Period after the first date on which the Contractor was required to provide the ISO Certificate in accordance with paragraph 0 (regardless of whether such failure is capable of remedy) shall constitute a Material Breach entitling the Authority to exercise its rights under clause F5.2A.

3.5 The Contractor shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within 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 0 to paragraph 0, the Authority may, in its absolute discretion, notify the Contractor that it is not in compliance with the Authority's Security Requirements and provide details of such non-compliance. The Contractor 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. For the avoidance of doubt, any failure to comply with the Authority's Security Requirements within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a Material Breach entitling the Authority to exercise its rights under clause F5.2A.

4. CYBER ESSENTIALS PLUS SCHEME

4.1 The Contractor 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 Contract Period. The Cyber Essentials Plus Certificate shall be provided by the Contractor to the Authority annually on the dates as agreed by the Parties.

4.2 The Contractor shall notify the Authority of any failure to obtain, or the revocation of, a Cyber Essentials Plus Certificate within 2 Working Days of confirmation of such failure or revocation. The Contractor shall, at its own expense, undertake those actions required in order to obtain a Cyber Essentials Plus Certificate following such failure or revocation. For the avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Plus Certificate during the Contract Period after the first date on which the Contractor was required to provide a Cyber Essentials Plus Certificate in accordance with paragraph 0 (regardless of whether such failure is

capable of remedy) shall constitute a Material Breach entitling the Authority to exercise its rights under clause F5.2A.

5. RISK MANAGEMENT

5.1 The Contractor shall operate and maintain policies and processes for risk management (the **Risk Management Policy**) during the Contract Period 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 Contractor shall provide the Risk Management Policy to the Authority upon request within 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 Contractor 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 Contractor shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Contractor's Systems Environment or in the threat landscape or (iii) at the request of the Authority. The Contractor shall provide the report of the Risk Assessment to the Authority, in the case of at least annual Risk Assessments, within 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 Contractor shall notify the Authority within 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 Contractor shall repeat the Risk Assessment within one calendar month of such request or as agreed by the Parties.

5.4 The Contractor 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 Contractor shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this paragraph 0. Any failure by the Contractor to comply with any requirement of this paragraph 0 (regardless of whether such failure is capable of remedy), shall constitute a Material Breach entitling the Authority to exercise its rights under clause F5.2A.

6. SECURITY AUDIT AND ASSURANCE

6.1 The Contractor 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 Contractor shall provide the completed Information Security Questionnaire to the Authority within one calendar month from the date of request.

6.2 The Contractor shall conduct Security Tests to assess the Information Security of the Contractor's Systems Environment and, if requested, the Authority's Systems Environment. In relation to such Security Tests, the Contractor 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 Contractor's Systems Environment or in the Authority's System Environment 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 Contractor 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 Contractor 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's Representative to witness the conduct of any Security Test. The Contractor shall provide to the Authority notice of any Security Test at least one month prior to the relevant Security Test.

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

6.5 Where the Contractor provides software development services, the Contractor 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 Contractor's Systems Environment after providing advance notice to the Contractor. If any Security Test identifies any non-compliance with the Authority's Security Requirements, the Contractor shall, at its own expense, undertake those actions required in order to rectify such identified noncompliance in the manner and timeframe as stipulated by the Authority at its absolute discretion. The Contractor 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 Contractor 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 Contractor 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 Contract Period 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 Contractor 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 Contractor shall provide the SOC1T2 report and SOC2T2 report to the Authority within 10 Working Days after receipt from its SOC Auditors.

6.10 In addition to the provisions set out in paragraphs 0 to 0, the Contractor 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 Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, attend.

7. PCI DSS COMPLIANCE AND CERTIFICATION

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

7.2 The Contractor 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 Contract Period. The Contractor shall provide the respective PCI Reports to the Authority upon request within 10 Working Days of such request.

7.3 The Contractor shall notify the Authority of any failure to obtain a PCI Report or a revocation of a PCI Report within 2 Working Days of confirmation of such failure or revocation. The Contractor 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 Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Security Policies and Standards set out 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 Contract Change, any change in the Authority's Security Requirements resulting from such Contract Change (if any) shall be agreed by the Parties in accordance with the Contract Change 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 agreed by the Parties and documented in the relevant Operational Change Confirmation.

8.3 The Contractor 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 Contractor shall be a member of the Cyber Security Information Sharing Partnership during the Contract Period. The Contractor shall participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information

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

ANNEX A – AUTHORITY SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-andstandards unless specified otherwise: a) Acceptable Use Policy

b) Information Security Policy

c) Physical Security Policy

d) Information Management Policy

e) Email Policy

f) Technical Vulnerability Management Policy

g) Remote Working Policy

h) Social Media Policy

i) Forensic Readiness Policy

j) SMS Text Policy

k) Privileged Users Security Policy

l) User Access Control Policy

m) Security Classification Policy

n) Cryptographic Key Management Policy

o) HMG Personnel Security Controls – May 2018 (published on https://www.gov.uk/government/publications/hmg-personnel-securitycontrols)

p) NCSC Secure Sanitisation of Storage Media (published on https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

ANNEX B – SECURITY STANDARDS

The Security Standards are published on:
https://www.gov.uk/government/publications/dwp-procurement-security-policies-andstandards:

a) SS-001 - Part 1 - Access & Authentication Controls
b) SS-001 - Part 2 - Privileged User Access Controls
c) SS-002 - PKI & Key Management
d) SS-003 - Software Development
e) SS-005 - Database Management System Security Standard
f) SS-006 - Security Boundaries
g) SS-007 - Use of Cryptography
h) SS-008 - Server Operating System
i) SS-009 - Hypervisor
j) SS-010 - Desktop Operating System
k) SS-011 - Containerisation
l) SS-012 - Protective Monitoring Standard for External Use
m) SS-013 - Firewall Security
n) SS-014 - Security Incident Management
o) SS-015 - Malware Protection
p) SS-016 - Remote Access
q) SS-017 - Mobile Devices
r) SS-018 - Network Security Design
s) SS-019 - Wireless Network
t) SS-022 - Voice & Video Communications
u) SS-023 - Cloud Computing
v) SS-025 - Virtualisation
w) SS-027 - Application Security Testing
x) SS-028 - Microservices Architecture
y) SS-029 - Securely Serving Web Content
z) SS-030 - Oracle Database aa) SS-031 - Domain Management bb) SS-033 - Patching

SCHEDULE 7 – SUSTAINABLE DEVELOPMENT REQUIREMENTS

Not Used

SCHEDULE 8 – LIFE CHANCES

Not Used

SCHEDULE 9 – WELSH LANGUAGE SCHEME

Not Used

SCHEDULE 10 – PARENT COMPANY GUARANTEE

Not Used

SCHEDULE 11 – CHANGE CONTROL PROCEDURE

1 General Principles of Change Control Procedure

1.1 This Schedule 11 sets out the procedure for dealing with Contract Changes and Operational Changes.

1.2 If either Party is in doubt about whether a change to the Contract falls within the definition of an Operational Change, it must be processed as a Contract Change.

1.3 For any Change Communication to be valid under this Schedule 11, it must be sent in accordance with the provisions of clause A5 (*Notices*) as if it were a notice.

2 Costs

2.1 The Contractor shall be entitled to increase the Contract Price only if the Impact Assessment satisfies the requirement in paragraph 5.2 of the Schedule 11, that the Contract Change is not exempt from a change in Contract Price as specified in clause F3 and it can demonstrate in the Impact Assessment that the proposed Contract Change requires additional resources and the Authority agrees to pay such increase.

2.2 The Contractor shall decrease the Contract Price if the Impact Assessment demonstrates that the proposed Contract Change would result in fewer resources being required to deliver the Services after that Contract Change is implemented than before that Contract Change is implemented.

2.3 Any change to the Contract Price resulting from a Contract Change, whether the change will cause an increase or a decrease in the Contract Price, will be strictly proportionate to the increase or decrease in the level of resources required for the provision of the Services affected by the change.

2.4 Each Parties' costs incurred in respect of any use of this Change Control Procedure as a result of any error or Default by the Contractor shall be paid for by the Contractor.

3 Operational Change Procedure

3.1 Any Operational Changes identified by either Party to improve operational efficiency of the Services may be implemented by the Contractor without following the Change Control Procedure provided they do not:-

(a) involve the Authority in paying any additional Contract Price or other costs;

(b) have an impact on the business of the Authority;

(c) require a change to this Contract; or

(d) have a direct impact on use of the Services.

3.2 Either Party may request an Operational Change by submitting an Operational Change Request to other Party at any time during the Contract Period, and which may be sent by electronic mail or by letter.

3.3 If the Party that receives an Operational Change Request wishes to agree to the Operational Change it must submit an Operational Change Confirmation to the other Party.

3.4 The Contractor shall inform the Authority of any impact on the Services that may arise from the proposed Operational Change.

3.5 The Contractor shall complete the Operational Change by the date agreed by the Parties in the Operational Change Confirmation and shall promptly notify the Authority when it is completed.

4 Contract Change Procedure

4.1 Either Party may issue a Change Request to the other Party at any time during the Contract Period. A Change Request shall be substantially in the form of Appendix 1 of this Schedule 11.

4.2 If the Authority issues a Change Request, then the Contractor shall provide as soon as reasonably practical, and in any event within three (3) Working Days of the date of receiving the Change Request, an Impact Assessment to the Authority.

4.3 If the Contractor issues the Change Request, then it shall provide an Impact Assessment to the Authority at the same time as the Change Request.

4.4 If the Contractor requires any clarification in relation to the Change Request before it can deliver the Impact Assessment, then it shall make a request for clarification to the Authority within three (3) Working Days of the date of receiving the Change Request.

4.5 Provided that sufficient information is received by the Authority to fully understand the nature of the request for clarification and the reasonable justification for the request, the time period to complete the Impact Assessment shall be extended by the time taken by the Authority to provide that clarification. The Authority shall respond to the request for clarification as soon as is reasonably practicable.

5 Impact Assessment

5.1 An Impact Assessment shall be substantially in the form of Appendix 2 of this Schedule 11.

5.2 Each Impact Assessment shall be completed in good faith and shall include:

(a) details of the impact the proposed Contract Change will have on the Services and the Contractor's ability to meet its other obligations under this Contract;

(b) any additional changes to the terms of this Contract that will be required as a result of that impact which may include changes to:-

(i) the Services and/or the Service Levels;

(ii) the format of Authority Data, as set out in the Services;

(iii) the Implementation Plan and any other timetable previously agreed by the Parties; and

(iv) other services provided by third party contractors to the Authority, including any changes required by the proposed Contract Change to the Authority's Systems Environment;

(c) a timetable for the implementation, together with any proposals for the testing of the Contract Change;

(d) details of how the proposed Contract Change will ensure compliance with any applicable change in Law which impacts on the performance of the Services which comes into force after the Commencement Date;

(e) any amendments to the Contract wording proposed in the Change Request Form;

(f) such other information as the Authority may reasonably request in (or in response to) the Change Request;

(g) details of the cost of implementing the proposed Contract Change; and

(h) details of any ongoing costs required by the proposed Contract Change when implemented, including any increase or decrease in the Contract Price, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party.

5.3 The calculation of costs for the purposes of paragraphs 5.2(g) and (h) of this Schedule 11 shall:

(a) include estimated volumes of each type of resource to be employed and the applicable rate card, where appropriate;

(b) include full disclosure of any assumptions underlying such Impact Assessment;

(c) include evidence of the cost of any assets required for the Change; and

(d) include details of any new Sub-contracts necessary to accomplish the Change.

5.4 If the Contract Change involves the processing or transfer of any Personal Data outside the European Economic Area, the preparation of the Impact Assessment shall also be subject to clause E2 (Protection of Personal Data).

5.5 Subject to the provisions of paragraph 5.6 of this Schedule 11, the Authority shall review the Impact Assessment and respond to the Contractor in accordance with paragraph 6 of this Schedule 11 within fifteen (15) Working Days of receiving the Impact Assessment.

5.6 If the Authority is the Receiving Party and the Authority reasonably considers that it requires further information regarding the proposed Contract Change so that it may properly evaluate the Change Request and the Impact Assessment or that a Change Request or Impact Assessment contains errors it shall notify the Contractor of this fact and detail any further information that it requires. The Contractor shall then re-issue the relevant Impact Assessment to the Authority within ten (10) Working Days of receiving such notification.

5.7 At the Authority's discretion, the Parties may repeat the process described in paragraph 5.6 of this Schedule 11 until the Authority is satisfied that it has sufficient information to properly evaluate the Change Request and Impact Assessment to enable it to take one of the steps prescribed by paragraph 6 of this Schedule 11.

6 Authority’s Right of Approval

6.1 Subject to paragraphs 5.6 and 5.7 of this Schedule 11, within fifteen (15) Working Days, or timescale agreed between both Parties, of receiving the Impact Assessment from the Contractor, the Authority shall do one of the following:

(a) approve the proposed Contract Change, in which case the Parties shall follow the procedure set out in paragraph 6.5 of this Schedule 11; or

(b) in its absolute discretion reject the Contract Change, in which case it shall notify the Contractor of the rejection. The Authority shall not reject any proposed Contract Change to the extent that the Contract Change

is necessary for the Contractor or the Services to comply with any changes in Law.

6.2 No proposed Contract Change shall be implemented by the Contractor until a Change Authorisation Note has been signed and issued by the Authority in accordance with paragraph 6.5 of this Schedule 11.

6.3 Unless the Authority expressly agrees (or requires) otherwise in writing, the Contractor shall continue to supply the Services in accordance with the existing terms of this Contract as if the proposed Contract Change did not apply.

6.4 Any discussions, negotiations or other communications which may take place between the Authority and the Contractor in connection with any proposed Contract Change, including the submission of any Change Communications, shall be without prejudice to each Party's other rights under this Contract.

6.5 If the Authority approves the proposed Contract Change pursuant to paragraph 6.1 of this Schedule 11 and it has not been rejected by the Contractor in accordance with paragraph 7 of this Schedule 11, then the Authority shall prepare two copies of a Change Authorisation Note in the form of Appendix 3 of this Schedule 11 and send them to the Contractor. The Contractor shall sign/executed as a deed (as appropriate) both copies and deliver both signed/executed copies to the Authority for its signature. Following receipt by the Authority of the Change Authorisation Note, it shall sign/seal (as appropriate) both copies and return one copy to the Contractor. On the Authority's signature the Change Authorisation Note shall constitute a binding change to this Contract.

7 Contractor's Right Of Rejection

7.1 Following an Impact Assessment, if the Contractor reasonably believes that any proposed Contract Change which is requested by the Authority would:

(a) materially and adversely affect the risks to the health and safety of any person; and/or

(b) require the Services to be performed in a way that infringes any Law,

7.2 then the Contractor shall be entitled to reject the proposed Contract Change and shall notify the Authority of its reasons for doing so within five (5) Working Days after the date on which it is obliged to deliver the Impact Assessment pursuant to paragraph 5.2 of this Schedule 11.

7.3 The Contractor shall have the right to reject a Change Request solely in the manner set out in paragraph 7.1 of this Schedule 11.

8 Failure to Comply

8.1 If the Contractor fails to complete an Impact Assessment, implement or successfully comply with the Contract Change by the required date, the Authority may:-

(a) give the Contractor a further opportunity to implement or comply with the Contract Change; or

(b) escalate any issues arising out of the failure to implement or comply with the Contract Change to the Contractor's finance director (or equivalent) under the dispute resolution procedure set out in clause I2 (Dispute Resolution).

8.2 If, despite the measures taken under paragraphs 8.1 (a) & 8.1(b) of this Schedule 11, the Contractor fails to implement or comply with the Contract Change, the Authority may elect to refer the matter for resolution by the dispute resolution procedure set out in clause I2 (Dispute Resolution).

9 Management Information

9.1 The Parties shall update the Contract to reflect all Contract Changes or Operational Changes agreed in the relevant Change Authorisation Note or Operational Change Request and annotate with a reference to the Change Authorisation Note or Operational Change Request pursuant to which the relevant Contract Changes or Operational Changes were agreed.

APPENDIX 1 - Change Request Form

(For Completion by the Party Requesting Change)

Change Request No:	Contract Title & Contract Number:	Contractor Name & Registered No:
Contract Change Title:	Contract Change Implementation Date:	
Full Description of Requested Contract Change (including proposed changes to wording of the Contract):		
Reasons for and Benefits of Requested Contract Change:		
Name of Owner Requesting Change:		
Signature of Owner Requesting Change:		
Date of Signature:		
(For Completion by Party Receiving Request for Change) Disadvantages of Requested Contract Change, if any:		
Details of any proposed alternative scenarios, if any;		
Authorisation to Complete Impact Assessment: (Name)		
Impact Assessment Assigned to: (Name)		
Impact Assessment Assigned on: (Date)		

APPENDIX 2 - Impact Assessment

(For Completion by DWP Contractor)

Change Request No:	Contract Title & Contract Number:	Contractor Name & Registered No:
Contract Change Title:	Contract Change Implementation Date:	
Full Details of the Impact the proposed Contract Change will have on the services and your ability to meet your other obligations under this Contract:		
Any additional changes to this Contract that will be required as a result of the change – including any: 1.Service/Service Levels/Performance Levels 2.Format of Authority Data 3.Timetable for the Implementation, including testing 4.Amendments to contract wording 5.Cost of implementing the change – ongoing/increase/decrease in costs 6.Alteration in Resources – estimated volumes and applicable rates		
Impact Assessment Completed by: (Name & Position in Organisation)		
(For Completion by DWP) Impact Assessment Approved by: (Name & Date)		
Impact Assessment Rejected by: (Name & Date)		
Reason For Rejection:		

APPENDIX 3 - Change Authorisation Note

(For Completion by DWP)

Change Request No:	Contract Title & Contract No:	Contractor Name & Registered No:
Contract Change Title:		Contract Change Implementation Date:
Detailed Description of Agreed Contract Change for which the Impact Assessment has been prepared. Provide details:		
Details of Agreed adjusted Contract Price resulting from the Contract Change for which the Impact Assessment has been prepared. Provide details:		
Amended/New Contract Wording – must include details of Cross Referencing to Original Contract Documents:		
In consideration of the rights and obligations created, granted and assumed by each Party to the other Party pursuant to this Change Authorisation Note, the Parties have agreed to enter into this Change Authorisation Note.		
The provisions of the Contract shall, save as amended in this Change Authorisation Note, continue in full force and effect, and shall be read and construed as one document with this Change Authorisation Note.		

Signed on Behalf of the Authority:	**Signed on Behalf of the Contractor:**
Signature:	Signature:
Name:	Name:
Position:	Position:
Date:	Date:

SCHEDULE 12 – PERSONAL DATA AND DATA SUBJECTS

The Parties are in agreement that the services being provided under this contract do not involve processing of personal data.