Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

Order Form

Call-Off Reference: Project 26246 Labour Market System data Migration, data access and database decommissioning.

Call-Off Title: RM1043.8 – Labour Market System data Migration, data access and database decommissioning.

Call-Off Contract Description: Labour Market System data Migration, data access and database decommissioning.

The Buyer: Department for Work and Pensions

Buyer Address: 2 St. Peter Square. Manchester. M2 3AA

The Supplier: **A&A Digital Tech Ltd**

Supplier Address: **310a First Floor, Station Road, Harrow, England, HA1 2DX**

Registration Number: **10236433**

DUNS Number: **221878311**

SID4GOV ID: **221878311**

Applicable Framework Contract

This Order Form is for the provision of the Call-Off Deliverables and dated 14th June 2024.

It's issued under the Framework Contract with the reference number RM1043.8 for the provision of Digital Outcomes Deliverables.

The Parties intend that this Call-Off Contract will not, except for the first Statement of Work which shall be executed at the same time that the Call-Off Contract is executed, oblige the Buyer to buy or the Supplier to supply Deliverables.

The Parties agree that when a Buyer seeks further Deliverables from the Supplier under the Call-Off Contract, the Buyer and Supplier will agree and execute a further Statement of Work (in the form of the template set out in Annex 1 to this Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules).

Upon the execution of each Statement of Work it shall become incorporated into the Buyer and Supplier's Call-Off Contract.

Call-Off Lot

RM1043.8 Digital Outcomes 6, Lot 1: Digital Outcomes

Call-Off Incorporated Terms

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

1 This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.

2 Joint Schedule 1 (Definitions) RM1043.8

3 Framework Special Terms

4 The following Schedules in equal order of precedence:

- Joint Schedules for RM1043.8
    - Joint Schedule 2 (Variation Form)
    - Joint Schedule 3 (Insurance Requirements)
    - Joint Schedule 4 (Commercially Sensitive Information)
    - Joint Schedule 6 (Key Subcontractors)
    - Joint Schedule 10 (Rectification Plan)
    - Joint Schedule 11 (Processing Data) RM1043.8 - As attached in this contract.

- Call-Off Schedules for RM1043.8
    - Call-Off Schedule 1 (Transparency Reports)
    - Call-Off Schedule 3 (Continuous Improvement)
    - Call-Off Schedule 5 (Pricing Details and Expenses Policy) - as attached in this contract
    - Call-Off Schedule 7 (Key Supplier Staff)
    - Call off Schedule 8 (Business Continuity and Disaster Recovery)
    - Call-Off Schedule 9 (Security) - as attached in this contract Security Long Form.
    - Call-Off Schedule 10 (exit Management)
    - Call-Off Schedule 15 (call off contract management)
    - Call-Off Schedule 18 (Background Checks)
    - Call-Off Schedule 20 (Call-Off Specification) - as attached in this contract
    - Call-Off Schedule 26 (Cyber Essentials Scheme)

5 CCS Core Terms (version 3.0.11)

6 Joint Schedule 5 (Corporate Social Responsibility) RM1043.8

7 Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above. (attached in this contract)

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

Call-Off Special Terms

The following Special Terms are incorporated into this Call-Off Contract:

- The Buyer shall advise the Supplier of any specific legal and regulatory requirements that are specific to the Buyer to which the Supplier must be aware of to enable it to provide the Services.
- The Parties agree that optional Call Off Schedule 2 (Staff Transfer) does not apply to this Call-Off Contract as there are no people in scope to transfer upon commencement of this Call-Off Contract.
- There are no Service Level Agreements, Liquidated Damages or Service Credits associated with this contract.
- DWP hybrid working policies will apply to any resource provided as part of this contract.
- DWP Offshoring Clauses: Protection on Information
    - The Contractor and any of its Sub-contractors, shall not access, process, host or transfer Authority Data outside the United Kingdom without the prior written consent of the Authority, and where the Authority gives consent, the Contractor shall comply with any reasonable instructions notified to it by the Authority in relation to the Authority Data in question. The provisions set out in this paragraph shall apply to Landed Resources.

- Where the Authority has given its prior written consent to the Contractor to access, process, host or transfer Authority Data from premises outside the United Kingdom: -

- a) the Contractor must notify the Authority (in so far as they are not prohibited by Law) where any Regulatory Bodies seek to gain or has gained access to such Authority Data;

- b) the Contractor shall take all necessary steps in order to prevent any access to, or disclosure of, any Authority Data to any Regulatory Bodies outside the United Kingdom unless required by Law without aany applicable exception or exemption

Call-Off Start Date: 24th June 2024

Call-Off Expiry Date: 23rd June 2026

Call-Off Initial Period: to be agreed in initial SOW

Call-Off Optional Extension Period: 12 months and 50% of contract maximum value

Minimum Notice Period for Extensions: 30 Days prior to the end of the initial contract period.

Call-Off Contract Value: Up to maximum value of £3,000,000.00 ex VAT (£3,600,000.00 including VAT) Any value commitment will be done through individual Statements of Work.

Call-Off Deliverables

Deliverables and outcomes will be agreed under separate SOWs and will be subject to the terms and conditions within this call off contract.

During the Call-Off Contract Period, the Buyer and Supplier may agree and execute completed Statement of Works. Upon execution of a Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

Buyer's Standards

From the Start Date of this Call-Off Contract, the Supplier shall comply with the relevant (and current as of the Call-Off Start Date) Standards referred to in Framework Schedule 1 (Specification).

Cyber Essentials Scheme

Cyber Essentials Plus

Maximum Liability

The limitation of liability for this Call-Off Contract is 150% of the Charges limited to the Statement of Work listed.

The Estimated Initial period charges used to calculate liability in the first Contract Year is £1,500,000 exclusive of VAT, £1,800,000 inclusive of VAT.

Call-Off Charges

Capped Time and Materials (T&M)

Reimbursable Expenses

DWP expenses must be pre agreed by individual project lead and be in line with the DWP

Travel & Expenses Policy. Supplier would not charge expenses for travel to main DWP Hub as specified below:

Working Age:

[REDACTED]

Payment Method

BACS - The Supplier will issue electronic invoices **monthly** in arrears. The Buyer will pay the Supplier within **30** days of receipt of a valid invoice.

This follows acceptance criteria being met in the method of weekly timesheet approval completed by the Buyer.

Suppliers must be prepared to use electronic purchase to pay (P2P) routes, including Catalogue and eInvoicing. Suppliers must be prepared to work with DWP to set up and test all electronic P2P routes. This may involve creating technical ordering and invoice files, including working with our ERP system service suppliers and systems.

Buyer's Invoice Address

[REDACTED]

Buyer's Authorised Representative

[REDACTED]

Buyer's Environmental Policy

Intentionally left blank

Buyer's Security Policy

Appended at Call-Off Schedule 9 (Security)

Additional DWP Security Clauses below:

The Supplier will ensure compliance with mandatory DWP security policies outlined below:

- AUTHORITY SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards 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/publica_tions/hmg-personnel-security-controls)

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

- SECURITY STANDARDS

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

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

SS-033 - Patching

Supplier's Authorised Representative

[REDACTED]

Supplier's Contract Manager

[REDACTED]

Key Staff

This information will be detailed in each individual SoW

Worker Engagement Route is inside of IR35 – Off-payroll working rules (IR35) apply.

Commercially Sensitive Information
Details of the Supplier's methodologies, policies and processes.

All information relating to limits of liability, daily fee rates, pricing and charging mechanisms contained in the Call-Off Contract.

The terms of the Supplier's insurance.
All details relating to personnel, including but not limited to the numbers of resources with specific skills, numbers of security cleared staff, staff terms and conditions of employment and staff selection methods.

Any information relating to other customers of the Supplier that has been obtained as a result of the Services or as a result of procuring the Services (including pre-contract references).

Additional Insurances

Not applicable

Guarantee

Not applicable

Social Value Commitment

Not applicable

Statement of Works :

During the Call-Off Contract Period, the Buyer and Supplier may agree and execute completed Statement of Works. Upon execution of a Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

Each signed Statement of Work will be automatically incorporated into this Order Form therefore does not require contract variation document. The SOW can be terminated for convenience by either party at 30 days notice.

For and on behalf of the Supplier:

Signature: [REDACTED]

Name: [REDACTED]

Role: [REDACTED]

Date:17/06/2024

For and on behalf of the Buyer:

Signature:

Name:

Role:

Date:

Annex 1 (Template Statement of Work)

1 Statement of Works (SOW) Details

Upon execution, this SOW forms part of the Call-Off Contract (reference below).

The Parties will execute a SOW for each set of Buyer Deliverables required. Any ad-hoc Deliverables requirements are to be treated as individual requirements in their own right and the Parties should execute a separate SOW in respect of each, or alternatively agree a Variation to an existing SOW.

All SOWs must fall within the Specification and provisions of the Call-Off Contact.

The details set out within this SOW apply only in relation to the Deliverables detailed herein and will not apply to any other SOWs executed or to be executed under this Call-Off Contract, unless otherwise agreed by the Parties in writing.

[REDACTED]

2 Call-Off Contract Specification – Deliverables Context

Name of Deliverable	Working Days	Day Rate	Total
See specific details in SOW 1 and resource table below		TBA	£XXXX (Exc VAT) £XXXX (Inc VAT) Including optional 91 Working Days £XXXX (Excl VAT) £XXXX (Incl VAT)

Security Applicable to SOW:

The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables, have completed Supplier Staff Vetting in accordance with Paragraph 6 (Security of Supplier Staff) of Part B – Annex 1 (Baseline Security Requirements) of Call-Off Schedule 9 (Security).

Cyber Essentials Scheme:

Required.

Additional Requirements:

1) The Supplier shall process Personal Data in accordance with Schedule 7 Annex 1 in the Call off Contract, with the 'Supplemental Information to Annex 1' (as set out below) and as agreed between the parties in any additional supplemental information to Annex 1 from time to time.

2) All Supplier resources will be inside IR35 in accordance with section 'Part A: Order Form' of the Call Off Contract. The Supplier confirms that all resources deployed to deliver the Services are PAYE and Tax and NI deductible at source.

3) All Supplier resources shall have BPSS level clearance at a minimum.

4) The majority of the Services will be delivered remotely. However, as some travel is required the applicable expenses including travel and accommodation as detailed below will be in line with the Buyer's policy on expenses detailed in the Call Off Contract and any travel that incurs expenses will be pre-approved by the Buyer.

Key Supplier Staff:

Resources as set out above all inside IR35

3 Charges

Call Off Contract Charges: £

[REDACTED]

Reimbursable Expenses:

DWP expenses must be pre agreed by individual project lead and be in line with the DWP Travel & Expenses Policy.

4 Signatures and Approvals

Agreement of this SOW

BY SIGNING this Statement of Work, the Parties agree that it shall be incorporated into Appendix 1 of the Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:

For and on behalf of the Supplier

Name: [REDACTED]

Title:

Date: 17/06/2024

Signature: [REDACTED]

For and on behalf of the Buyer

Name: [REDACTED]

Title: Commercial Lead

Date: XXXX

Signature: XXXX

Annex 1

Data Processing

Prior to the execution of this Statement of Work, the Parties shall review Annex 1 of Joint Schedule 11 (Processing Data) and if the contents of Annex 1 does not adequately cover the Processor / Controller arrangements covered by this Statement of Work, Annex 1 shall be amended as set out below and the following table shall apply to the Processing activities undertaken under this Statement of Work only:

Description	**Details**
Identity of Controller for each Category of Personal Data	1. The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: a. business contact details of Supplier Staff for which the Supplier is the Controller; and b. business contact details of any members of the public, directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Staff) for which the Buyer is the Controller. 2. Buyer shall be a Controller for the purposes of Data Protection Legislation in respect of: a. opinions and responses provided (including any special category personal data that may be collected) during any research activity by: i. directors, officers, employees, agents, consultants and contractors of Buyer; and ii. members of the public.
Duration of the Processing	The duration of the Call-Off Contract

Nature and purposes of the Processing	Supplier Processing Supplier Processing – is as set out broadly in the SOW's but is limited to viewing of, and consulting in relation to, personal data. The parties agree that: 1. The Supplier will follow the Buyer's direction and guidelines on staff security Buyer systems, including role-based access controls and security standards. Where the Supplier is required to grant user access, this will be undertaken at the Buyer's direction. 2. Access for the Supplier to Buyer systems will be limited to Buyer provisioned laptops and approved USB devices. 3. Any requirement to share data externally, such as with third parties for diagnostic purposes, is not to be undertaken by the Supplier and will remain the responsibility of the Buyer.
Type of Personal Data	1. Contact information (e.g. business e-mail address, telephone number etc.). 2. Personal life information (e.g. life habits, family situation). 3. Employment information (e.g. position, experience or employment history). 4. Identification information (e.g. name, gender, image in communication systems, benefit case reference information). 5. Data concerning health. 6. Data revealing racial or ethnic origin.
Categories of Data Subject	1. Any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Staff) for which the

	Buyer is the Controller 2. Members of the general public 3. Supplier Staff engaged in the performance of the Supplier's duties under the SoW for which the Supplier is the Controller.
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	Delete or return as directed by the Buyer

Contract Schedules:

Call-Off Schedule 4 (Call-Off Tender)

Response Template:

[REDACTED]

[REDACTED]

[REDACTED]

Call-Off Schedule 5 (Pricing Details and Expenses Policy)

Call-Off Contract Charges

1.1 The Supplier shall provide:

1.1.1 as part of the Further Competition Procedure, its pricing for the Deliverables is in accordance with the Buyer's Statement of Requirements.

1.1.2 for each individual Statement of Work (SOW), the applicable Charges shall be calculated in accordance with the Pricing Mechanisms detailed in the Order Form using all of the following:

(a) the agreed rates for Supplier Staff and/or facilities (which are exclusive of any applicable expenses and VAT) incorporated into the Call-Off Contract; and

(b) the number of Work Days, or pro rata portion of a Work Day (see Paragraph 2.3.1 of Framework Schedule 3 (Framework Pricing)), that Supplier Staff work solely to provide the Deliverables and/or the provision of facilities solely to be used for the Buyer's stated purposes of providing the Deliverables and to meet the tasks sets out in the SOW between the SOW Start Date and SOW End Date.

1.2 Further to Paragraph 2.2.2 of Framework Schedule 3 (Framework Pricing), the Supplier will provide a detailed breakdown of its Charges for the Deliverables in sufficient detail to enable the Buyer to verify the accuracy of any invoice submitted.

This detailed breakdown will be incorporated into each SOW and include (but will not be limited to):

- a role description of each member of the Supplier Staff;
- a facilities description (if applicable);
- the agreed day rate for each Supplier Staff;
- any expenses charged for each Work Day for each Supplier Staff, which must be in accordance with the Buyer's expenses policy (if applicable);
- the number of Work Days, or pro rata for every part day, they will be actively be engaged in providing the Deliverables between the SOW Start Date and SOW End Date; and
- the total SOW cost for all Supplier Staff role and facilities in providing the Deliverables.

1.3 If a Capped or Fixed Price has been agreed for a particular SOW:

- the Supplier shall continue to work on the Deliverables until they are satisfactorily complete and accepted by the Buyer at its own cost and expense where the Capped or Fixed Price is exceeded; and
- the Buyer will have no obligation or liability to pay any additional Charges or cost of any part of the Deliverables yet to be completed and/or Delivered after the Capped or Fixed Price is exceeded by the Supplier.

1.4 All risks or contingencies will be included in the Charges. The Parties agree that the following assumptions, representations, risks and contingencies will apply in relation to the Charges:

Annex 1 (Expenses Policy)

Reimbursable Expenses

It is not anticipated that the Supplier will claim travel and subsistence expenses and in the even that any expenses are claimed, these will be payable based on the conditions below:

be based on actuals and

not include any Supplier travel between Supplier to Supplier sites;

not include any Supplier travel to DWP main hubs defined in Call Off Buyer Location

have the Buyer's prior agreement and electronic e-mail consent by the Buyer.

not exceed DWP policy (DWP Supplier Travel Policy-Jan-23.pdf, attached here).


DWP Supplier Travel Policy - Jan 23.pdf

It is expected that the Supplier rates provided in the table below will not increase for the contract duration for any reason. Any additional rates supplied for other roles will be aligned to SFIA rate card.

[REDACTED]

Call-Off Schedule 9 (Security)

~~Part A: Short Form Security Requirements~~

~~Definitions~~

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

~~Term~~	~~Definition~~
~~Breach of Security~~	~~the occurrence of:~~ (a) ~~any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or~~ (b) ~~the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,~~ ~~in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with Paragraph 2.2; and~~
~~Security Management Plan~~	~~the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated~~

	from time to time.

Complying with security requirements and updates to them

1.2 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

1.3 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

1.4 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

1.5 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

1.6 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

Security Standards

1.7 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

1.8 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

1.8.1 is in accordance with the Law and this Contract;

1.8.2 as a minimum demonstrates Good Industry Practice;

1.8.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

1.8.4 where specified by the Buyer in accordance with Paragraph 2.2 complies with the Security Policy and the ICT Policy.

1.9 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

1.10 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

~~Security Management Plan~~

1.11 **~~Introduction~~**

1.11.1 ~~The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.~~

1.12 **~~Content of the Security Management Plan~~**

1.12.1 ~~The Security Management Plan shall:~~

(a) ~~comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;~~

(b) ~~identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;~~

(c) ~~detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;~~

(d) ~~be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;~~

(e) ~~set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;~~

(f) ~~set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with Paragraph 2.2 the Security Policy; and~~

(g) ~~be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.~~

1.13 **~~Development of the Security Management Plan~~**

1.13.1 ~~Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.~~

1.13.2 ~~If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved,~~

the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

1.13.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

1.13.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

1.14 **Amendment of the Security Management Plan**

1.14.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Deliverables and/or associated processes;

(c) where necessary in accordance with Paragraph 2.2, any change to the Security Policy;

(d) any new perceived or changed security threats; and

(e) any reasonable change in requirements requested by the Buyer.

1.14.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

(a) suggested improvements to the effectiveness of the Security Management Plan;

(b) updates to the risk assessments; and

(c) suggested improvements in measuring the effectiveness of controls.

1.14.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

1.14.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

Security breach

1.15 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

1.16 Without prejudice to the security incident management process, upon becoming aware

~~of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:~~

1.16.1 ~~immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:~~

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

(b) ~~remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;~~

(c) ~~prevent an equivalent breach in the future exploiting the same cause failure; and~~

(d) ~~as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.~~

1.17 ~~In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with Paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.~~

~~Data security~~

1.18 ~~The Supplier will ensure that any system on which the Supplier holds any Government Data will be accredited or assured as specific to the Buyer and will comply with:~~

- ~~the Government Security Policy Framework (see: https://www.gov.uk/government/publications/security-policy-framework);~~
- ~~the Government Functional Standard GovS 007: Security (see: https://www.gov.uk/government/publications/government-functional-standard-govs-007-security); and~~
- ~~guidance issued by the National Cyber Security Centre (NCSC) for:~~
  - ~~risk management: https://www.ncsc.gov.uk/collection/risk-management-collection;~~
  - ~~cloud security: https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles; and~~
  - ~~10 steps to cyber security: https://www.ncsc.gov.uk/collection/10-steps.~~

1.19 ~~Where the duration of a Call-Off Contract exceeds one (1) year, the Supplier will review the accreditation or assurance status at least once each year to assess whether material changes have occurred which could alter the original accreditation decision in relation to Government Data. If any changes have occurred then the Supplier agrees to promptly re-submit such system for re-accreditation.~~

Part B: Long Form Security Requirements

Definitions

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

Term	Definition

Breach of Security	means the occurrence of: (a) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or (b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;
ISMS	the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and
Security Tests	tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

Security Requirements

1.2 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

1.3 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

1.4 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

1.4.1 Tracy Butters DWP Security

1.4.2 **Neeraj Dad**

1.5 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

1.6 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

1.7 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.

1.8 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

1.9 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

Information Security Management System (ISMS)

1.10 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.

1.11 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

1.12 The Buyer acknowledges that;

1.12.1 If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and

1.12.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.

1.13 The ISMS shall:

1.13.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;

1.13.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;

1.13.3 at all times provide a level of security which:

(a) is in accordance with the Law and this Contract;

(b) complies with the Baseline Security Requirements;

(c) as a minimum demonstrates Good Industry Practice;

(d) where specified by a Buyer that has undertaken a Further Competition, complies with the Security Policy and the ICT Policy;

(e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1 to 4) (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework);

(f) takes account of guidance issued by the Centre for Protection of National Infrastructure (https://www.cpni.gov.uk);

(g) complies with HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm);

(h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

(i) addresses issues of incompatibility with the Supplier's own organisational

security policies; and

(j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

1.13.4 document the security incident management processes and incident response plans;

1.13.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

1.13.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

1.14 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

1.15 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

1.16 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

1.17 Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

Security Management Plan

1.18 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

1.19 The Security Management Plan shall:

1.19.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);

1.19.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;

1.19.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

1.19.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;

1.19.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

1.19.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);

1.19.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

1.19.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

1.19.9 set out the scope of the Buyer System that is under the control of the Supplier;

1.19.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

1.19.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

1.20 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this

Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

1.21 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

Amendment of the ISMS and Security Management Plan

1.22 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:

1.22.1 emerging changes in Good Industry Practice;

1.22.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;

1.22.3 any new perceived or changed security threats;

1.22.4 where required in accordance with paragraph 3.4.3 (d), any changes to the Security Policy; and

1.22.5 any reasonable change in requirement requested by the Buyer.

1.23 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

1.23.1 suggested improvements to the effectiveness of the ISMS;

1.23.2 updates to the risk assessments;

1.23.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

1.23.4 suggested improvements in measuring the effectiveness of controls.

1.24 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.

1.25 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

Security Testing

1.26 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief

against any resultant under-performance for the period of the Security Tests.

1.27 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.

1.28 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

1.29 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

1.30 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

Complying with the ISMS

1.31 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.

1.32 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.

1.33 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

Security Breach

1.34 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

1.35 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

1.35.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

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

(b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;

(c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

(d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

(e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

(f) as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

1.36 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

Vulnerabilities and fixing them

1.37 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

1.38 The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

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

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

1.39 The Supplier shall procure the application of security patches to vulnerabilities within a

maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

1.39.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

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

1.39.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

1.40 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

1.40.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

1.40.2 is agreed with the Buyer in writing.

1.41 The Supplier shall:

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

1.41.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

1.41.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

1.41.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;

1.41.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

1.41.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

1.41.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and

1.41.8 inform the Buyer when it becomes aware of any new threat, vulnerability or

exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

1.42 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

1.43 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B: Annex 1

Baseline security requirements

Handling Classified information

1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

End user devices

1.2 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre (“NCSC”) to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").

1.3 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a ‘known good’ state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

Data Processing, Storage, Management and Destruction

1.4 The Supplier and Buyer recognise the need for the Buyer’s information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

1.5 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

1.6 The Supplier shall:

1.6.1 provide the Buyer with all Government Data on demand in an agreed open format;

1.6.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

1.6.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

1.6.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

Ensuring secure communications

1.7 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.

1.8 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

Security by design

1.9 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

1.10 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (https://www.ncsc.gov.uk/section/products-services/ncsc-certification) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

Security of Supplier Staff

1.11 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

1.12 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

1.13 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.

1.14 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

1.15 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

Restricting and monitoring access

1.16 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and

administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

Audit

1.17 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

1.17.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

1.17.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

1.18 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

1.19 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B: Annex 2

Security Management Plan

Joint Schedule 11 (Processing Data) RM1043.8

Definitions

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

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

Status of the Controller

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

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

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

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

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

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

Where one Party is Controller and the other Party its Processor

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

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

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

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

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

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

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

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

7 Process that Personal Data only in accordance with Annex 1 (Processing Personal Data), unless the Processor is required to do otherwise by Law. If it is so required the

Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

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

9 nature of the data to be protected;

10 harm that might result from a Personal Data Breach;

11 state of technological development; and

12 cost of implementing any measures;

13 ensure that:

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

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

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

b. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

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

d. have undergone adequate training in the use, care, protection and handling of Personal Data;

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

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

18 the Data Subject has enforceable rights and effective legal remedies;

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

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

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

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

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

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

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

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

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

28 becomes aware of a Personal Data Breach.

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

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

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

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

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

34 assistance as requested by the Controller following any Personal Data Breach; and/or

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

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

37 the Controller determines that the Processing is not occasional;

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

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

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

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

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

43 notify the Controller in writing of the intended Subprocessor and Processing;

44 obtain the written consent of the Controller;

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

46 provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

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

48 The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

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

1 Where the Parties are Joint Controllers of Personal Data

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

1 Independent Controllers of Personal Data

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

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

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

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

55 The Parties shall only provide Personal Data to each other:

56 to the extent necessary to perform their respective obligations under the Contract;

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

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

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

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

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

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

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

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

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

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

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

68 implement any measures necessary to restore the security of any compromised Personal Data;

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

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

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

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

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

1 Annex 1: Processing Personal Data

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

a. The contact details of the Relevant Authority's Data Protection Officer are:

[REDACTED]

b. The contact details of the Supplier's Data Protection Officer are: [REDACTED]

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

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

Description	**Details**
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with Paragraph 3 to Paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: • **Citizen Names** • **Citizen Addresses** • **Citizen National Insurance Number**
Duration of the Processing	17th June 2024 – 16th June 2026 – the duration of the contract
Nature and purposes of the Processing	First Phase only Moving data from the existing, non-cloud hosted legacy system to the target cloud hosted replacement systems so DWP agents maintain access to LMS data. Other phases to be assessed at another time
Type of Personal Data	PII Data : Names, addresses and National Insurance Numbers of citizens
Categories of Data Subject	360 Table name fields and 4239 data items get completed by staff covering all aspects of a claimant (and partners) interaction with the jobcentre agent. [REDACTED]
Plan for return and destruction of the data once the Processing is complete	No requirement for Supplier to hold, store data themselves as they are expected to utilise DWP devices and hosting services to carry out their work throughout

UNLESS requirement under Union or Member State law to preserve that type of data	

1 ~~Annex 2: Joint Controller Agreement~~

1 ~~Joint Controller Status and Allocation of Responsibilities~~

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

f. ~~The Parties agree that the **[Supplier/Relevant Authority]:**~~

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

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

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

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

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

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

1 ~~Undertakings of both Parties~~

b. ~~The Supplier and the Relevant Authority each undertake that they shall:~~

80 ~~report to the other Party every 3 months on:~~

81 ~~the volume of Data Subject Access Requests (or purported Data Subject Access~~

~~Requests) from Data Subjects (or third parties on their behalf);~~

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

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

84 ~~any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and~~

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

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

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

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

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

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

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

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

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

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

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

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

96 ~~nature of the data to be protected;~~

97 ~~harm that might result from a Personal Data Breach;~~

98 ~~state of technological development; and~~

99 ~~cost of implementing any measures;~~

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

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

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

1 Data Protection Breach

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

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

103 all reasonable assistance, including:

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

105 co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

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

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

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

108 the nature of the Personal Data Breach;

109 the nature of Personal Data affected;

110 the categories and number of Data Subjects concerned;

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

112 measures taken or proposed to be taken to address the Personal Data Breach; and

113 describe the likely consequences of the Personal Data Breach.

1 Audit

a. The Supplier shall permit:

114 the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

1

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

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

1 Impact Assessments

b. The Parties shall:

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

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

1 ICO Guidance

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

1 Liabilities for Data Protection Breach

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

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

118 if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant

Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

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

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

a. If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("**Court**") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

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

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

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

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

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

1 Termination

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

1 Sub-Processing

b. In respect of any Processing of Personal Data performed by a third party on

behalf of a Party, that Party shall:

124 carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

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

1 Data Retention

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

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract.

Labour Market System data migration and data access

SPECIFICATION

Procurement Reference No:	**Project_26246**

Requirements

Buyer Details	
Buyer:	DWP Digital
Function/Team:	Universal Credit / Working Age
Principle Contact Name:	[REDACTED]
Principle Contact email:	[REDACTED]
Principle Contact Role:	Lead Delivery Manager / Senior Product Manager

Contractual Details	
Title of Requirement:	Labour Market System data migration and data access
Brief Description of Requirement:	To migrate data from the legacy Labour Market System (LMS) database and enable DWP agent access from modern UI's developed elsewhere in DWP. In addition, this requirement may also extend to provide a store for that data, facilitate access to that data [by DWP Agents], and decommissioning of the current database.

Anticipated Start Date:	01/05/2024
Location	United Kingdom DWP Leeds hub is base location for the work, however buyer operates hybrid working arrangements [currently 40% office attendance for DWP personnel] DWP doesn't mandate supplier attendance in the DWP location.
Buyer's equipment	Use of buyer's equipment is mandatory.
Cloud Services	
=	

DWP is developing several new digital solutions to provide replacement functionality for the legacy Labour Market System (LMS). These replacement services will be hosted in the cloud.

These new digital solutions will provide services for storing new business data, which would otherwise be stored in the legacy Labour Market system, but themselves do not provide the data migration capability to copy data from the legacy system to the replacement services and may not facilitate full access to all the data that has to be migrated.

The data migration and access services to be procured under this agreement would facilitate migration to the cloud by moving data from the existing, non-cloud hosted legacy system to the target cloud hosted replacement systems so DWP agents maintain access to LMS data from other DWP Services (User Interfaces)

If required the buyer may also commission under this agreement the creation of a datastore for this data (if it isn't provided by other DWP services) and may also commission the full decommissioning of the legacy LMS database once the work is complete.

Background and Context

Why the work is being done: This needs to be clear and give some background as to why this work/service is needed. Describe the organisation or policy goal the work supports. You must say if you need the work to be done by a certain date, this will help understand any time constraints.

The Labour Market System (LMS) is an incumbent legacy system used primarily in Job Centres to record and manage interactions between DWP and claimants.

The buyer has an urgent requirement to migrate any required active and historical data to an alternative store so that DWP agents can continue to access it without the need to use the LMS. Data migration target completion date is February 2025.

An alternative database will be required to host the migrated data and the Buyer intends to provide this, however if it isn't available in time the Buyer may commission the supplier to develop such a database.

The buyer also plans to develop services to allow DWP Agents to access the migrated data without the need to use the existing LMS service. If these services aren't ready in time the Buyer will commission the Supplier to provide a means to access the migrated data through a simplified browser-based User Interface to DWP standards.

Objective and Vision

Problem to be solved: You must be clear on what problem suppliers will be solving and the desired final outcome. Detail the key success factors the contract will contribute to achieving.

Data Migration

A data migration process is required so that a large volume of data can be automatically extracted from the legacy Labour Market System and copied in to target replacement digital solutions which are currently in development internally by DWP.

The data migration process should:

- Target only the data residing in the source legacy system that is required by DWP operations and service staff.
- Run either continually or at regular intervals so that data entered into the legacy system can be synchronised with the target replacement digital services (until such time as DWP disables further updates to data in the legacy service).

The desired outcome is for all required data to have been copied from the legacy system to the target replacement digital solutions so that the legacy system is no longer required to access and update that data.

Database

DWP currently plans to provide a Database within its existing Evergreen Infrastructure from which services like Managing Working Age Customers (MWAC), Support Offers and New Style Benefits will extract, use, update, maintain and delete data previously migrated from LMS. However, in the event that this Database isn't created in time or is unable to store all the migrated data that DWP Agents require access then the supplier will be asked to provide a Database solution within DWP's Cloud Hosted Services (for ongoing support by DWP.

Data Access

A separate data access requirement may also be commissioned from the supplier under this work. Currently DWP expects to provide full access to the migrated LMS data through new services it is developing called Managing Working Age Customers (MWAC), Support Offers and New Style Benefits. These services are in various states of design, build, deployment and operation. These new services should meet the data access requirement within the timeframe of this contract however, in circumstances where this isn't possible or where Managing Working Age Customers (MWAC), Support Offers and New Style Benefits don't provide access to some migrated LMS data then an simplified browser based user interface to access that data would also need to be provided by the Supplier.

Database Decommissioning

Following the migration and withdrawal of LMS service from DWP agents the department intends to fully decommission the LMS Service database. DWP may require the supplier to engage with the existing service provider to ensure decommissioning is completed in accordance with DWP guidelines.

Statement of Requirements

Requirement

The Requirements are divided into four elements, data migration service, database creation, data access and database decommissioning. DWP intends to commit initially to progress the migration element of the requirement, subsequent Statements of Work will be commissioned for the remaining three elements if required.

Data Migration Service

- Produce a targeted database data migration technical solution design specification based upon the DWP business data definitions of the data to be migrated from the Labour Market System (LMS),
- Develop a data extract process to iteratively locate the required data in the source Oracle database, transform it into the data format required by the target replacement digital solutions and send the data to the target systems, being developed by DWP, though REST Application Programming Interface (API) requests.
- Provide a data extract process that either:
    - Operates in batches that are resumable and can be started and stopped at any time
    - Operates continuously to stream data from the source database to the target systems in real-time
- Respond to requests from DWP for any additional data items that are identified for migration and incorporate in to the solution.
- Provide end-to-end testing, support and bugfixes of the developed data migration solution until all required has been migrated to target systems.
- The data migration process must be able to handle new records being added to the source database and include any new records within the migration process.
- The data migration process must have as minimal change as possible to the source system.
- The data migration process must be appropriately performance optimised and rate limited to avoid adversely impacting the performance of either the source or target systems.
- The data migration solution must be deployed to DWP Universal Credit/Working Age managed cloud infrastructure and adhere to DWP engineering, infrastructure and application deployment standards.

Database Creation

- If specified provide Database solution within DWP's Cloud Hosted Services (for ongoing support by DWP.

Data Access

- If specified produce a targeted data access technical solution design specification based upon the DWP business needs of the migrated data that is not otherwise accessible through new DWP Services.
- If specified design, build and deploy a data access solution so that it meets DWP business needs for access to migrated data that is not otherwise accessible through new DWP services.

Database decommissioning

- engage with the existing service provider to ensure decommissioning is completed in accordance with DWP guidelines

Exit / Future Requirements
Outline how you plan to exit and transition from this contract following expiry any detail any potential future requirements that may replace it.

- DWP personnel must be trained to maintain and enhance developed source code
- DWP personnel must be able to support the services through its managed cloud infrastructure
- The supplier must fully document their adherence to DWP engineering, infrastructure and application deployment standards including those related to the support and maintenance of the resulting services according to its Technology Services standards.
- DWP must retain ownership of developed source code.

Key Deliverables / Outcomes

First element only – Data Migration Services

- Database data migration technical solution design specification
- Publish a review of the DWP business data definitions of the data to be migrated from the Labour Market System (LMS) – in preparation for a migration
- Document a data extract process that clearly shows how supplier will iteratively locate the required data in the source Oracle database, transform it into the data format required by the target replacement digital solutions and send the data to the target systems, being developed by DWP, though REST Application Programming Interface (API) requests.
- End to End test results that show conclusively the supplier can
    - Provide a data extract process that either:
        - Operates in batches that are resumable and can be started and stopped at any time
        - Operates continuously to stream data from the source database to the target systems in real-time
    - Respond to requests from DWP for any additional data items that are identified for migration and incorporate in to the solution.
    - Provide end-to-end testing, support and bugfixes of the developed data migration solution until all required has been migrated to target systems.
- Completion statement demonstrating achievement of the SRE on-boarding criteria and achievement of Technical Services Service standards [SG1 and SG2] for the respective Supplier delivered services

Subsequent Phases (if commissioned) - detail and deliverables to be agreed before Statement of Works are signed

- a database solution provisioned within DWP Working Age Evergreen infrastructure
- a targeted data access technical solution design specification based upon the DWP business needs of the migrated data that is not otherwise accessible through new DWP Services.
- a functioning data access solution that meets DWP business needs for access to migrated data that is not otherwise accessible through new DWP services.
- Confirmation of LMS database decommission in accordance with DWP Standards and guidelines

Standards

Quality standards	As specified by DWP Digital and CDDO Digital Service Standards

Technical standards:	As specified by DWP Technical Design Authority Standard As specified by DWP Security Standards

Personal Data and Data Subjects - GDPR Information		
Will Supplier Have Access To Personal Data?		**x** Yes No
Identity of Controller for each Category of Personal Data		**To be defined and agreed during the project as required.** x The Buyer is Controller and the Supplier is Processor The Supplier is Controller and the Buyer is Processor The Parties are Joint Controllers
Duration of the Processing	Up to 7 years after the expiry or termination of this Call-Off Contract.	
Nature and purposes of the Processing	First Phase only Moving data from the existing, non-cloud hosted legacy system to the target cloud hosted replacement systems so DWP agents maintain access to LMS data. Other phases to be assessed at another time.	
Type of Personal Data	Personal Identifiable Information (PII) data	
Categories of Data Subject	360 Table name fields and 4239 data items get completed by staff covering all aspects of a claimant (and partners) interaction with the jobcentre agent. [REDACTED]	
Plan for return and destruction of the data	No requirement for Supplier to hold, store data themselves as they are expected to utilise DWP	

once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	devices and hosting services to carry out their work throughout.

Worker Engagement Route (including IR35 status)

Where the Buyer has assessed its requirement and it is for resource, the IR35 status of the Supplier Staff in Key Roles must be detailed in this Specification and, if applicable, in each Statement of Work.