SCHEDULE 7B

Order Form for Competed Goods, - Device Support and Request Services, Mini Competition

Call-Off Contract under the HealthTrust Europe LLP Framework Agreement for the provision of Enterprise Level Information Communication Technology (ICT) Solutions for hardware, software, programs, applications, security, computer science, managed services, consultancy, support and associated services – 2019 (reference number: SF050716) dated 27th September 2019.

The Authority	The Secretary of State for The Department of Work & Pensions, Caxton House, Tothill Street, London, SW1H9NA
The Supplier	CDW Limited, One New Change, London, EC4M 9AF
HealthTrust Europe Contract Reference	HTE-005703

The Supplier and the Authority hereby agree as follows:

1. Following the completion of a mini-competition exercise ("**Mini-Competition**") for the 'Device Support and Request Services, the Authority wishes to enter into a Contract in respect of the Services pursuant to the Framework Agreement.

2. The Contract incorporates, and the Supplier agrees to abide by, the following documents:

   (a) the Mini-Competition Specification of the Authority's requirements as appended at Appendix 1 overleaf;

   (b) the Call-Off Terms and Conditions set out at Appendix A, as applicable, to the Framework Agreement (including the front page and all Schedules thereto);

(c) the Department of Works and Pensions Security Schedule ("**DWP Security Schedule**"), as appended at Appendix 13 overleaf;

(d) the terms of the Software and End User License Agreement (EULA) as appended at Appendix 9 overleaf;

(e) the DWP standard GDPR terms and conditions as appended at Appendix 14 overleaf; and

(f) The Information Security Questionnaire in the format stipulated by the Authority as appended at Appendix 16 overleaf.

3. In the event of (and only to the extent of) any conflict between the DWP standard terms and conditions; the terms of the Software and End User Licence Agreement (EULA); the DWP Security Schedule and the terms and conditions of the Authority's Mini-Competition Specification; the Mini-Competition Response Document; and the Call-off Terms and Conditions set out at Appendix A, the following order of precedence shall apply:

(a) Schedule 7B Order Form Framework Agreement;

(b) the Appendix A Call-off Terms and Conditions.

(c) the Authority's Mini-Competition Specification; and

(d) the Supplier's Mini Competition Response Document;

(e) the terms of the Software and End User License Agreement (EULA);

4. Where the Call-Off Terms and Conditions set out at Schedule 1 of Appendix A to the Framework Agreement apply, the Authority acknowledges and agrees to the HealthTrust Europe Key Provisions, in particular, as stated below for the avoidance of doubt:

(a) In the event that the Authority terminates its agreement with HealthTrust Europe (made pursuant to the provisions of the UHCW Framework) for convenience or otherwise, and such termination takes effect before the end of the Initial Term (as defined in the UHCW Framework) or in the event that the Authority's agreement with HealthTrust Europe (made pursuant to the provisions of the UHCW Framework) expires without being renewed on or

after such Initial Term, HealthTrust Europe shall notify the Supplier of such termination or expiry in accordance with the provisions of Clause 16 of Schedule 1 of the Framework Agreement ("**Beneficiary Withdrawal Notice**"). Upon receipt of such Beneficiary Withdrawal Notice by the Supplier, the Supplier shall cease to apply for the benefit of the Authority, the Contract Price or any special discounts in relation to such supply which applied solely by reason of the operation of the UHCW Framework and its associated services and/or framework agreements or any contract made between the Authority made pursuant thereto and further the Authority shall no longer be permitted to place Orders or benefit from the Contract Price, save with the prior written consent of HealthTrust Europe.

(b) The Authority acknowledges and agrees that the Supplier is subject to an activity-based income (ABI) management charge in relation to any Orders placed by the Authority under the Framework Agreement.

5. Key Contract Dates

For the avoidance of doubt the Parties agree to the following:

(a) this agreement shall start from the date the Authority Representative signs this Order Form (hereinafter "the Commencement Date"). The period following the Commencement Date shall constitute the Implementation Period. The Term of the Implementation Period shall be a period agreed between the Parties, as laid out in Appendix 4.

(b) The Supplier shall commence in delivering Services agreed under the contract on a date mutually agreed between the Parties (hereinafter the "Actual Services Commencement Date").

(c) For avoidance of doubt, the Actual Services Commencement Date shall only commence after the Implementation Period ends. For the avoidance of doubt the Supplier shall not deliver any Services under the Contract during the Implementation Period.

(d) The Initial Term of this Call-Off Contract shall be 24 months from the Actual Services Commencement Date.

(e) The Supplier will carry out the Implementation obligations stated under Appendix 4 subject to payment of transition charges to the Supplier by

the Authority as part of the Milestone payments stated under clause 3.1 of Appendix 4. The parties acknowledge and agree that any charges submitted by the Supplier to the Authority have been based on the Authority providing accurate and complete information to the Supplier based on Authority's specification and responses to Supplier's due diligence enquiries. Accordingly, subject to Supplier not incurring any extra costs due to Authority's negligence, inaccuracies, acts or omissions, any such resulting costs to be chargeable to the Authority, Supplier will carry out Implementation obligations not priced under the transition charges, at Supplier's own cost.

6. The Parties agree that any monetary values stipulated by the Authority does not commit the Authority to any spend under the contract, but is a reflection of the anticipated spend limit the Authority applies to the contract, upon full performance of the Supplier's Service delivery obligations.

7. Data Protection

(a) The Parties acknowledge that the Authority is the Data Controller (as defined by the Data Protection Legislation) and the Supplier is the Data Processor (as defined by the Data Protection Legislation) in respect of any Personal Data ("**Authority Data**") Processed under this Contract.

(b) The Supplier shall only Process Authority Data (in accordance with the standard GDPR terms and conditions .

(c) The Supplier shall and will also ensure that any Sub-contractor (as applicable) shall, complete the Information Security Questionnaire in the format stipulated by the Authority and appended at Appendix 16 at least annually or at the request by the Authority. The Supplier shall provide the completed Information Security Questionnaire to the Authority within one calendar month from the date of request.

(d) The Supplier 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 Supplier 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.

(e) The Parties acknowledge that Schedule 3 of the Call-off Terms and Conditions, 'Information and Data provisions', clause 2.6 shall be deleted and not apply for the purposes of the Contract. The following clause shall apply

instead and Supplier's liability shall be capped, notwithstanding the references in Schedule 2 of the Call-off Terms and Conditions, clause 12.2 to the deleted clause 2.6 having unlimited liability. Supplier's liability for unlawful or unauthorised Processing, destruction and/or damage to Personal Data in connection with the GDPR terms and conditions and this Contract shall be subject to the following capped liability:

"Supplier's aggregate liability under the Contract for any loss, damages, costs, expenses (including without limitation legal costs and expenses), claims or proceedings whatsoever or howsoever arising from the Supplier's unlawful or unauthorised Processing, destruction and/or damage to Personal Data in connection with this Contract shall not exceed £8,000,000 (Eight Million Pounds),

(f) Where the Authority has given its prior written consent to the Supplier to access, process, host or transfer Authority Data from premises outside the United Kingdom (in accordance with clause 7(d) of the Contract):

i. the Supplier must notify the Authority (in so far as Suppliers are not prohibited by Law) where any Regulatory Bodies seek to gain or has gained access to such Authority Data;

ii. the Supplier 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 any applicable exception or exemption.

8. The payment profile for this Contract shall be within 30 days of receipt of an accepted invoice for the performance of the Contract.

9. The Authority may terminate this Contract forthwith by notice in writing to the Supplier for any reason and at any time on three (3) month′s written notice.

10. The Contract Managers at the commencement of this Contract are:
for the Authority: **Redacted**
for the Supplier: **Redacted**

11. Notices served under this Contract are to be delivered to:

a) for the Authority: **Redacted,** Department of Work and Pensions, Finance Group, Second Floor Shell Area Yellow Zone, Peel Park Control Centre,

Blackpool Industrial Estate, FY4 5ES. Notices will also be sent via e-mail to **Redacted** and ED.DESKTOPBAG@DWP.GOV.UK

b) for the Supplier: Head of Legal, CDW Limited, One New Change, London, EC4M 9AF and legal@uk.cdw.com

12. In this Contract, unless the context otherwise requires, all capitalised words and expressions shall have the meanings ascribed to them by the Framework Agreement and/ or Call-Off Terms and Conditions.

13. Use of Suppliers

Save for Data Processing obligations, the Authority grants permission for the Supplier to Sub-contract any of its obligations under this Framework Agreement which shall not be unreasonably withheld. The Supplier shall stipulate all subcontracting partners in Appendix 11.

14. Supplier Periodic Assessment of Call off Contract Charges and Savings

(a) Within the first 11 months of the Actual Services Commencement Date the Supplier shall be obliged to:

(a)(i) notify the Authority of a recommended independent market data source (or sources) of data relating to the charges and costs for provision of the same or similar services in the UK (the "Benchmark Data".)

(a)(ii) Work with the Authority to agree the final independent source of the Benchmark Data to be used within 10 working days of the Supplier's recommendation.

(b) Starting from the Actual Services Commencement Date, the Supplier shall continue to perform a benchmarking exercise every twelve (12) months during the Term (or in the event that such dates do not, in any Contract Year, fall on a Working Day, on the next Working Day following such dates).

(c) The Supplier shall utilise the Benchmark Data to compare the cost of contract against market value rates, to assess whether:

(c)(i) the Supplier is able to reduce its Call Off Contract Charges; and

(c)(ii) Charges under the Call off contract continues to offer value for money outcomes to the department.

(d) To the extent that the Benchmark Data indicates that the Supplier is able to decrease all or part of the Call Off Contract Charges or that all or part of the Contract no longer represents value for money it shall promptly notify the Authority in writing and a Call Off Contract Charge reduction shall be implemented or an alternative cost reduction solution acceptable to the Authority shall be put in place.

(e) The Supplier shall provide the Authority a written copy of the Benchmark Data and any supporting evidence used by the Supplier in reaching a conclusion as per clause 14(c).

15. Dispute resolution

(a) The Parties shall resolve Disputes arising out of or in connection with this Call Off Contract in accordance with the Dispute Resolution Procedure outlined in Section 22 of Appendix A of the framework agreement.

(b) The Supplier shall continue to provide the Services in accordance with the terms of this Call Off Contract until a Dispute has been resolved.

16. Records, Audit Access

a) The Supplier shall:

i) keep the records and accounts in accordance with Good Industry Practice and Law; and

ii) afford any Auditor access to the records and accounts at the Supplier's premises and/or provide records and accounts (including copies of the Supplier's published accounts) or copies of the same, as may be required by any of the Auditors from time to time during the Call Off Contract Period, in order that the Auditor(s) may carry out an inspection to assess compliance by the Supplier and/or its Sub-Contractors of any of the Supplier's obligations under this Call Off Contract Agreement including for the following purposes to:

(1) verify the accuracy of the Call Off Contract Charges and any other amounts payable by the Authority under this Call Off Contract (and any

proposed or actual variations to them in accordance with this Call Off Contract);

(2) verify the costs of the Supplier (including the costs of all Sub-Contractors and any third party suppliers) in connection with the provision of the Services;

(3) verify the Supplier's and each Sub-Contractor's compliance with the applicable Law;

(4) identify or investigate an actual or suspected Prohibited Act, impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Authority shall

(5) have no obligation to inform the Supplier of the purpose or objective of its investigations;

(6) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, the Call Off Guarantor and/or any Sub-Contractors or their ability to perform the Services;

(7) obtain such information as is necessary to fulfil the Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General;

(8) review any books of account and the internal contract management accounts kept by the Supplier in connection with this Call Off Contract;

(9) carry out the Authority's internal and statutory audits and to prepare, examine and/or certify the Authority's annual and interim reports and accounts;

(10) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;

(11) verify the accuracy and completeness of any information delivered or required by this Call Off Contract;

(12) inspect the Information & Computer Technology (ICT) Environment (or any part of it) and the wider service delivery environment (or any part of it);

(13) review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;

(14) review the Supplier's quality management systems (including all relevant Quality Plans and any quality manuals and procedures);

(15) review the Supplier's compliance with the Standards;

(16) inspect the Authority Assets, including the Authority's IPRs, equipment and facilities, for the purposes of ensuring that the Authority Assets are secure and that any register of assets is up to date; and/or

(17) review the integrity, confidentiality and security of the Authority Data.

b) The Authority shall mutually agree timescales to ensure that the conduct of each audit does not unreasonably disrupt the Supplier or delay the provision of the Services save insofar as the Supplier accepts and acknowledges that control over the conduct of audits carried out by the Auditor(s) is outside of the control of the Authority.

c) Subject to the Supplier's rights in respect of Confidential Information, the Supplier shall on demand provide the Auditor(s) with all reasonable co-operation and assistance in:

i) all reasonable information requested by the Authority within the scope of the audit;

ii) reasonable access to sites controlled by the Supplier and to any Supplier Equipment used in the provision of the Services; and

iii) access to the Supplier Personnel.

d) The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under this clause, unless the audit reveals a Default by the Supplier in which case the Supplier shall

reimburse the Authority for the Authority's reasonable costs incurred in relation to the audit.

17. Exit Plan

a) An Exit Plan shall be developed by the Supplier and provided to the Authority within three (3) months of the Commencement Date, as stipulated in Clause 15.9, Schedule 2 of the Appendix A Framework Agreement.

18. Termination Assistance

a) The Authority shall be entitled to require the provision of Termination Assistance during the Call Off Contract Period by giving written notice to the Supplier (a "Termination Assistance Notice") at two (2) months prior to the Call Off Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

i) the date from which Termination Assistance is required;

ii) the nature of the Termination Assistance required; and

iii) the period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) months after the date that the Supplier ceases to provide the Services.

b) The Authority shall have an option to extend the Termination Assistance Period beyond the period specified in the Termination Assistance Notice provided that such extension shall not extend for more than six (6) months after the date the Supplier ceases to provide the Services or, if applicable, beyond the end of the Termination Assistance Period and provided that it shall notify the Supplier to such effect no later than twenty (20) Working Days prior to the date on which the provision of Termination Assistance is otherwise due to expire. The Authority shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier to such effect.

19. Termination Assistance Period

a) Throughout the Termination Assistance Period, the Supplier shall:

(i) continue to provide the Services (as applicable);

(ii) in addition to providing the Services and the Termination Assistance, provide to the Authority any reasonable assistance requested by the Authority to allow the Services to continue without interruption following the termination or expiry of this Call Off Contract and to facilitate the orderly transfer of responsibility for and conduct of the Services to the Authority and/or its Replacement Supplier;

(iii) mutually agree timescales to reallocate resources to provide such assistance as is referred to in paragraph 21(a)(ii) of this Call Off Schedule without additional costs to the Authority;

(iv) provide the Services and the Termination Assistance at no detriment to the Service Level Performance Measures, save to the extent that the Parties agree otherwise in accordance with paragraph 21(c); and

b) Without prejudice to the Supplier's obligations under paragraph 21(a)(iii) of this Call Off Schedule, if it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in paragraph 21(a)(ii) of this Call Off Schedule without additional costs to the Authority, any additional costs incurred by the Supplier in providing such reasonable assistance which is not already in the scope of the Termination Assistance or the Exit Plan shall be subject to the Change Control Process.

c) If the Supplier demonstrates to the Authority's reasonable satisfaction that transition of the Services and provision of Termination Assistance during the Termination Assistance Period will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Level Performance Measure(s), the Parties shall vary the relevant Service Level Performance Measure(s) and/or the applicable Service Credits to take account of such adverse effect.

20. Termination Obligations

(a) The Supplier shall comply with all of its obligations contained in the Exit Plan.

(b) Upon termination or expiry (as the case may be) or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Services and the Termination Assistance and its compliance with the other provisions of this Call Off Schedule), the Supplier shall:

(i) cease to use the Authority Data;

(ii) provide the Authority and/or the Replacement Supplier with a complete and uncorrupted version of the Authority Data in electronic form (or such other format as reasonably required by the Authority);

(iii) erase from any computers, storage devices and storage media that are to be retained by the Supplier after the end of the Termination Assistance Period all Authority Data and promptly certify to the Authority that it has completed such deletion;

(iv) return to the Authority such of the following as is in the Supplier's possession or control:

(A) all copies of the Authority Software and any other software licensed by the Authority to the Supplier under this Call Off Contract;

(B) all materials created by the Supplier under this Call Off Contract in which the IPRs are owned by the Authority;

(C) any parts of the ICT Environment and any other equipment which belongs to the Authority;

(D) any items that have been on-charged to the Authority, such as consumables; and

(E) all Authority Property issued to the Supplier. Such Authority Property shall be handed back to the Authority in good working order (allowance shall be made only for reasonable wear and tear);

(F) any sums prepaid by the Authority in respect of Services not Delivered by the Call Off Expiry Date;

(c) vacate any Authority Premises;

(d) remove the Supplier Equipment together with any other materials used by the Supplier to supply the Services and shall leave the Sites in a clean, safe and

tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier and/or any Supplier Personnel;

(e) provide access during normal working hours to the Authority and/or the Replacement Supplier for up to twelve (12) months after expiry or termination to:

(i) such information relating to the Services as remains in the possession or control of the Supplier; and

(ii) such members of the Supplier Personnel as have been involved in the design, development and provision of the Services and who are still employed by the Supplier, provided that the Authority and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to requests for access under this paragraph.

(f) Upon termination or expiry (as the case may be) or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Services and the Termination Assistance and its compliance with the other provisions of this Call Off Schedule), each Party shall return to the other Party (or if requested, destroy or delete) all Confidential Information of the other Party and shall certify that it does not retain the other Party's Confidential Information save to the extent (and for the limited period) that such information needs to be retained by the Party in question for the purposes of providing or receiving any Services or Termination Services or for statutory compliance purposes.

(g) Except where this Call Off Contract provides otherwise, all licences, leases and authorisations granted by the Authority to the Supplier in relation to the Services shall be terminated with effect from the end of the Termination Assistance Period.

21. In relation to the Appendices:

Appendix 1	Mini-Competition Specification
Appendix 2	Mini-Competition Response Document
Appendix 3	Change Control Process
Appendix 4	Implementation Plan
Appendix 5	Locations subject to lease and/or licence
Appendix 6	Step In Rights
Appendix 7	Termination Sum
Appendix 8	TUPE Staff Transfer
Appendix 9	Software and End User License Agreement (EULA)
Appendix 10	SLAs + KPIs + XLAs + Reporting
Appendix 11	Subcontractor Information
Appendix 12	DWP Additional Clauses
Appendix 13	DWP Security Schedule
Appendix 14	DWP GDPR Clauses
Appendix 15	Data Protection Protocol
Appendix 16	DWP Information Security Questionnaire
Appendix 17	Governance
Appendix 18	Invoicing
Appendix 19	Definitions

(a) The Supplier shall implement the Services in accordance with the Implementation Plan appended at Appendix 4 overleaf.

(b) Any changes to this Contract, including to the Services and Goods, may only be agreed in accordance with the Change Control Process set out in Appendix

3 overleaf.

(c) Notwithstanding Key Provision 8 of the Call-Off Terms and Conditions, the Parties agree that the commencement of the provision of the Goods under this Contract shall give rise to a relevant transfer as defined in TUPE and therefore the provisions of Appendix 8 shall apply to such transfer.

(d) If the Supplier is unable to provide the Services, then the Authority shall be entitled to exercise Step In Rights set out in Appendix 6. The Authority shall procure that any person appointed by the Authority under Appendix 6 shall be subject to duties of confidentiality substantially similar to those described in Schedule 3 of the Call-off Terms and Conditions, 'Information and Data Provisions', clause 1.

(e) The warranty for Goods and end user license agreement (EULA) applicable to the relevant Product, is as stipulated by the Manufacturer of that Product appended at Appendix 9.

(f) The KPI's, SLA and Service Credits applicable to the Contract are detailed in Appendix 10.

(g) The bidding model that includes members of the supply chain, the percentage of work being delivered by each Sub-contractor and the key contract deliverables for which each Sub-contractor will be responsible are detailed in Appendix 11.

Signed by the authorised representative of THE AUTHORITY

Name:	**Redacted**	Signature:	**Redacted**.....
Position:	**Redacted** **.....**		

Signed by the authorised representative of THE SUPPLIER

Name:	**Redacted** **.....**	Signature	……**Redacted**…… ……
Position:	…**Redacted**…… ……		

Appendix 1

Mini Competition Device Services Specification

DSRS Requirements
Specification Final.doc

Included in Addendum 1

Appendix 2

Mini Competition Response Document

Included in Addendums:

Addendum 2: **Redacted** Commercial Response

Addendum 3: **Redacted** Technical Response

Addendum 4: **Redacted** Response Clarifications

The pricing model selected for the Device & Monitor Repair & Replace service will be a Fixed Price arrangement based upon the tender submission. The Authority reserves to right to vary that model in the future and will enter into good faith negotiations with the supplier to see if varying the model provides best value for money and improved delivery of services.

In respect of the prices provided for Request Management Non Standard, Request Management Projects and Bulk Transformation it is recognized that the pricing provided at the tender process, embedded, were based upon scenarios and not actual quantities for evaluation purposes. These prices will be used for benchmarking purposes for any future activity that the Authority may contract with the Supplier.

Appendix 3

Change Control Process

The Contract can be varied only by a change control note, defined under Section 42 of Appendix A Call-off Terms and Conditions, which explicitly states it is intended to vary this Contract, and which is signed by an authorised representative of each Party. Each Party may from time to time notify the other in writing as to who is the point of receipt of that notification and an authorised representative for that Party.

Change%20Control%20Forms%20-%20IC1

Included in Addendum 5

Appendix 4

Implementation Plan

1. Formation of Enactment of the Implementation Plan

1.1. An Implementation Plan (or parts thereof) shall be provided in draft by the Supplier prior to the Commencement Date, the Supplier's draft must contain information at the level of detail necessary to manage the implementation stage effectively and as the Authority may require. The draft Implementation Plan shall take account of all dependencies known to, or which should reasonably be known to the Supplier. Where the draft plan cannot be made available prior to the Commencement Date, both parties agree that it shall be made available within 10 working days of contract signature.

1.2. The Supplier's Implementation Plan must contain information at the level of detail necessary and shall include as a minimum the following:

1.2.1. People

1.2.2. Processes

1.2.3. Tooling

1.2.4. Testing

1.3. The Supplier shall submit the draft Implementation Plan to the Authority for Approval (such decision of the Authority to Approve or not shall not be unreasonably delayed or withheld).

1.4. The Supplier shall agree its final Implementation Plan with the Authority within ten (10) Working days after the Commencement Date. Where the draft plan cannot be made available prior to the Commencement Date, both parties agree that it shall be made available within 10 working days of contract signature.

1.5. The Supplier shall perform each of the Deliverables identified in the Implementation Plan by the applicable date assigned to that Deliverable in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is Achieved on or before its Milestone Date.

1.6. The Supplier shall monitor its performance against the Implementation Plan and Milestones and any other requirements of the Authority as set out in the Order Form and report to the Authority on such performance.

2. Control of Implementation Plan

2.1. Subject to Clause 2.2, the Supplier shall keep the Implementation Plan under review in accordance with the Authority's instructions and ensure that it is maintained and updated on a regular basis as may be necessary to reflect the then current state of the provision of the Services. The Authority shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

2.2. Changes to the Milestones (if any), Milestone Payments (if any) and Delay Payments (if any) shall only be made by the Authority in accordance with the Change Control Process and provided that the Supplier shall not attempt to postpone any of the Milestones using the Variation Procedure or otherwise (except in the event of an Authority Cause which affects the Supplier's ability to achieve a Milestone by the relevant Milestone Date).

2.3. Failure of the Supplier to provide a draft Implementation Plan on time shall be a material Default unless the parties expressly agree otherwise or the failure is as a result of an Authority Cause.

2.4. Without prejudice to 2.3. should Supplier fail to provide the draft Implementation Plan on time, the parties may consider using dispute resolution procedures as a means to remedy the issues in a timely manner as articulated under Clause 22 of Schedule 2 of the Call Off Terms and Conditions. For the avoidance of doubt, if Supplier fails to provide a draft Implementation Plan on time material Default shall apply if not resolved through dispute resolution procedures.

3. Implementation Period

3.1. The Authority will not remunerate the Supplier for Service Costs during the Implementation Period, which is expected to be no more than a 3-month period from commencement. The Supplier will be awarded Milestone payments relating to completion of agreed Implementation Milestones.

3.2. The Authority shall report Service Level Agreements (SLAs), Experience Level Agreements (XLAs), or Key Performance Indicators (KPIs) throughout the term of the Implementation Period as agreed between the parties. The Authority will not apply Service Credits throughout the Term of the Implementation Period.

3.3. The Supplier shall monitor and maintain the Implementation Plan in line with requirements stipulated in Appendix 4.

3.4. For the avoidance of doubt, this agreement shall start from the date the Authority signs this Order Form (hereinafter "the Commencement Date"). The period following the Commencement Date shall constitute the Implementation Period. The Term of the Implementation Period shall be a period agreed between the Parties, as laid out in Appendix 4.

3.5. For the avoidance of doubt, delivery of Services shall begin on the Actual Services Commencement Date. For avoidance of doubt, the Actual Services Commencement Date will commence after the Implementation Period ends as agreed between the parties. The Term of this Call-Off Contract shall be 24 months from the Actual Services Commencement Date.

4. Rectification of Delay in Implementation

4.1. If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Call Off Contract:

4.2. it shall:

4.2.1. notify the Authority as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay; and

4.2.2. include in its notification an explanation of the actual or anticipated impact of the Delay and provide a remediation plan to rectify the Delay; and

4.2.3. comply with the agreed remediation plan as provided by the Supplier in order to address the impact of the Delay or anticipated Delay; and use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay; and if the Delay or anticipated Delay relates to a Milestone in respect which a Delay Payment has been specified in the Implementation Plan, Clause 5 (Delay Payments) shall apply.

5. Delay Payments

5.1. If Delay Payment mechanisms have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Supplier shall pay to the Authority such Delay Payments (calculated as set out by the Authority in the Implementation Plan) and the following provisions shall apply:

5.1.1.the Supplier acknowledges and agrees that any Delay Payment is a price adjustment and not an estimate of the Loss that may be suffered by the Authority as a result of the Supplier's failure to Achieve the corresponding Milestone;

5.1.2. Delay Payments shall be the Authority's exclusive financial remedy for the Supplier's failure to Achieve a corresponding Milestone by its Milestone Date except where: the Authority is otherwise entitled to or does terminate this Call Off Contract; or

Appendix 5

Lease and/or Licence to access Premises and Locations

Not Used in this Contract.

Appendix 6

Step In Rights

1. The Authority may take action under this clause in the following circumstances:

1.1. the Authority is entitled under this section to terminate the Call-Off Contract in accordance with Clause 15.4 of the Call-Off Terms and Conditions set out in Appendix A.

1.2. there is a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any part thereof;

1.3. there is a Delay that has or the Authority reasonably anticipates will result in the Supplier's failure to Achieve a Milestone in respect of Authority to Proceed by its Milestone Date;

1.4. a Force Majeure Event occurs which materially prevents or materially delays the performance of the Services or any part thereof;

1.5. the Supplier has failed any single SLA in three (3) consecutive reporting periods;

1.6. where the Supplier is not in Default of its obligations under this Agreement but the Authority considers that the circumstances constitute an emergency;

1.7. where a Regulatory Body has advised the Authority that the exercise by the Authority of its rights under this clause is necessary;

1.8. because a serious risk exists to the health or safety of persons, property or the environment;

1.9. to discharge a statutory duty;

1.10. on the occurrence of an Insolvency Event in respect of the Supplier; and/or

1.11. where it is required to do so by the Framework Authority.

Action to be taken before the exercise of the right of Step-in

1.12. Before the Authority exercises its right of step-in under this clause it shall permit the Supplier the opportunity to demonstrate to the Authority's reasonable satisfaction within ten (10) Working Days of the step in right arising that the Supplier is still able to provide the Services in accordance with the terms of this Agreement and/or remedy the circumstances giving rise to the right to step-in without the requirement for the Authority to take action.

1.13. If the Authority is not satisfied with the Supplier's demonstration pursuant to Clause 1.12, the Authority may:

1.14. where the Authority considers it expedient to do so, require the Supplier by notice in writing to take those steps that the Authority considers necessary or expedient to mitigate or rectify the state of affairs giving rise to the Authority's right to step-in;

1.15. appoint any person to work with the Supplier in performing all or a part of the Services (including those provided by any Sub-contractor); or

1.16. take the steps that the Authority considers appropriate to ensure the performance of all or part of the Services (including those provided by any Sub-contractor).

1.17. The Supplier shall cooperate fully and in good faith with the Customer Authority, or any other person appointed in respect of Clause 1.15 and shall adopt any reasonable methodology in providing the Services recommended by the Authority or that person.

Exercise of the right of Step-in

1.18. If the Supplier fails to:

1.18.1. confirm within three (3) Working Days of a notice served that it is willing to comply with that notice;

1.18.2.work with a person appointed in accordance with Clause 1.15; or

1.18.3.take the steps notified to it by the Authority,

then the Authority may take action under this clause.

1.19. If the Authority takes action pursuant to Clause 1.18, the Authority shall serve written notice ("Step-In Notice") on the Supplier. The Step-in Notice shall set out the following:

1.19.1.the action the Authority wishes to take and in particular the Services it wishes to control;

1.19.2.the reason for and the objective of taking the action and whether the Authority reasonably believes that the primary cause of the action is due to the Supplier's Default;

1.19.3.the date it wishes to commence the action;

1.19.4.the time period which it believes will be necessary for the action;

1.19.5.whether the Authority will require access to the Supplier's premises and/or the Sites; and

1.19.6.to the extent practicable, the effect on the Supplier and its obligations to provide the Services during the period the action is being taken.

1.20. Following service of a Step-in Notice, the Authority shall:

1.20.1.take the action set out in the Step-in Notice and any consequential additional action as it reasonably believes is necessary (together, the "Required Action");

1.20.2.keep records of the Required Action taken and provide information about the Required Action to the Supplier;

1.20.3.cooperate wherever reasonable with the Supplier in order to enable the Supplier to continue to provide any Services in relation to which the Authority is not assuming control; and

1.21. take such steps as are reasonably open to it to limit the amount of the cost that the Supplier shall incur as a result of the exercise of the Customer Authority's rights under this clause (provided that this does not prejudice achievement of the Authority's objectives).

1.22. For so long as and to the extent that the Required Action is continuing, then the Supplier shall:

1.23. cooperate fully with the Authority to facilitate the steps taken;

1.24. suspend performance of the Services subject to the step-in rights (the "Step-In Services") to the extent that the Authority so requests for the purposes of its exercise of step-in rights, provided always that the exercise of the step-in right shall not excuse the Supplier from its obligation to provide the Services (excluding the Step-In Services for the period only of exercise of the step-in right) in accordance with this Agreement or be deemed to frustrate or waive performance of that obligation;

1.25. grant and procure that any Sub-contractor or relevant third party grants such licences and permissions as are reasonably required provided that these are no more expensive than the charges that would have been payable by the Supplier; and

1.26. afford (and procure that its Sub-contractors afford as applicable) to the Authority such cooperation, access to and use of (as applicable):

1.27. the Supplier Assets and Authority Assets used to provide the Services and other goods and services used to provide the Services;

1.28. all necessary and associated documentation relating to those Supplier Assets and Authority Assets used by the Supplier to provide the Services to the Authority and any other goods and services used to provide the Services so as to enable the same to be operated;

1.29. the Supplier’s Intellectual Property Rights used in relation to the Services; and

1.30. premises, equipment, personnel, documents, information or other items as are reasonably required.

1.31. For so long as and to the extent that the Required Action is continuing, then:

1.32. the Supplier shall not be obliged to provide the Services to the extent that they are the subject of the Required Action;

1.33. the Authority shall pay to the Supplier the Charges after deduction of any applicable Service Credits, Delay Payments and the Customer Authority’s reasonable and direct costs of taking the Required Action. If the Supplier retains partial responsibility for a Service, then the reduction in Charges shall be proportionate to the reduction in the Supplier’s responsibility.

1.34. If the Required Action results in:

1.34.1.the degradation of any Services not subject to the Required Action; or

1.34.2.the non-Achievement of a Milestone,

1.34.3.beyond that which would have been the case had the Authority not taken the Required Action, then the Supplier shall be entitled to an agreed adjustment of the Charges, provided that the Supplier can demonstrate to the reasonable satisfaction of the Authority that the Required Action has led to the degradation or non-Achievement.

1.35. Before ceasing to exercise its step-in rights under this Clause the Authority shall deliver a written notice to the Supplier ("Step-Out Notice"), specifying:

1.36. the Required Action it has actually taken; and

1.37. the date on which the Authority plans to end the Required Action ("Step-Out Date") subject to the Authority being satisfied with the Supplier's

ability to resume the provision of the Services and the Supplier's plan developed.

1.38. The Supplier shall, following receipt of a Step-Out Notice and not less than twenty (20) Working Days before the Step-Out Date, develop for the Customer Authority's Approval a draft plan ("Step-Out Plan") relating to the resumption by the Supplier of the Services, including any action the Supplier proposes to take to ensure that the affected Services satisfy the requirements of this Agreement.

1.39. If the Authority does not Approve the draft Step-Out Plan, the Authority shall inform the Supplier of its reasons for not approving it. The Supplier shall then revise the draft Step-Out Plan taking those reasons into account and shall re-submit the revised plan to the Authority for the Authority's Approval. The Authority shall not withhold or delay its Approval of the draft Step-Out Plan unnecessarily.

1.40. The Supplier shall bear its own costs in connection with any step-in by the Authority under this clause provided that the Authority shall reimburse the Supplier's reasonable additional expenses incurred directly as a result of any step-in action taken by the Authority under:

1.41. Clauses 1.4 or 1.7; or

1.42. Clauses 1.8, 1.9 and 1.10 provided that the primary cause of the Authority serving the Step-In Notice was not a Supplier's Default.

Appendix 7

Termination Sum

No Termination Sum shall apply in this Contract other than the obligation to exchange reasonable consideration related to delivered Goods and Services completed in accordance with the delivery dates and prices set out in the Mini Competition Response Document in Appendix 2.

Appendix 8

TUPE Staff Transfer

Schedule 7 of the NHS Terms and Conditions for the Provision of Services (Contract Version) (December 2016) is incorporated into this Order Form. Where any term used is not defined within the Call-off Terms and Conditions, such term shall have the meaning given within such Schedule 7.

The following parts of Schedule 7 shall not be used for the purposes of this Order Form:

- Part A- No staff transfer to the Supplier under TUPE
- Part B- Staff transfer from the Authority under TUPE

The following parts of Schedule 7 shall be used for the purposes of this Order Form:

- Part C- Staff transfer from a current provider under TUPE

The parties agree that the provisions of Part C shall apply as amended as follows:

Clause 1.7 shall be deleted and replaced with the following:

1.7 The Authority shall procure that the relevant Third Party will indemnify and keep indemnified the Supplier in relation to any Employment Liabilities arising out of or in connection with any claim arising from:

1.7.1 the Third Party's (or any sub-contractor of the Third Party's) failure to perform and discharge its obligations to provide, no later than twenty eight (28) days prior to the Transfer Date, a final list to the Supplier containing the names of all the Third Party Employees whom the Third Party (or any subcontractor of the Third Party) expects will transfer to the Supplier and all employee liability information identified in regulation 11 of TUPE in relation to the Third Party Employees;

1.7.2 any act or omission by the Third Party (or any sub-contractor of the Third Party) in respect of the Third Party Employees occurring on or before the Transfer Date;

1.7.3 any allegation or claim by any person who is not a Third Party Employee but who alleges that their employment should transfer or has transferred to the Supplier (or any Sub-contractor, as appropriate);

1.7.4 any emoluments payable to a person employed or engaged by the Third Party (or any sub-contractor of the Third Party) (including without limitation all wages, accrued holiday pay, bonuses, commissions, PAYE, national insurance contributions, pension contributions and other contributions) payable in respect of any period on or before the Transfer Date;

1.7.5 any allegation or claim by any of the Third Party Employees on the grounds that the Supplier or Sub-contractor, as appropriate, has failed to continue a benefit provided by the Third Party as a term of such Third Party Employee's contract as at the Transfer Date where it was not reasonably practicable for the Supplier or Sub-contractor, as appropriate, to provide an identical benefit but where the Supplier or Sub-contractor, as appropriate, has provided (or offered to provide where such benefit

is not accepted by the Third Party Employee) an alternative benefit which, taken as a whole, is no less favourable to such Third Party Employee; and

1.7.6 any act or omission of the Third Party (or any sub-contractor of the Third Party) in relation to its obligations under regulation 13 of TUPE, or in respect of an award of compensation under regulation 15 of TUPE except to the extent that the liability arises from the Supplier's, or Sub-contractor's, failure to comply with regulation 13(4) of TUPE.

New clauses 1.8 and 1.9 shall be added as follows:

1.8 The Authority shall procure that the relevant Third Party will indemnify and keep indemnified the Supplier and any Sub-contractor, as applicable, in respect of any Employment Liabilities arising from any act or omission of the Third Party (or any sub-contractor of the Third Party) in relation to any other employee, agent, consultant and/or contractor of the Third Party (or sub-contractor of the Third Party) who is either partially or fully engaged in the performance of the Services who is not a Third Party Employee arising during any period whether before, on or after the Subsequent Transfer Date.

1.9 If any employee of a Third Party who is not identified as a Transferring Third Party Employee and claims, and/or it is determined, in relation to such person that his/her contract of employment has been transferred from a Third Party to the Supplier and/or any Notified Sub-contractor pursuant to the Employment Regulations then:

1.9.1 the Supplier will within 5 Working Days of becoming aware of that fact notify the Authority and the relevant Third Party in writing;

1.9.2 the Third Party may offer employment to such person, or take such other steps as it considers appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Supplier;

1.9.3 if such offer of employment is accepted, the Supplier shall immediately release the person from its employment;

1.9.4 if after the period referred to in Paragraph 1.9.2 no such offer has been made, or such offer has been made but not accepted, the Supplier may within 5 Working Days give notice to terminate the employment of such person;

and subject to the Supplier's compliance with Paragraphs 1.9.1 to 1.9.4 the Authority shall procure that the Third Party will indemnify the Supplier and/or the relevant Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any of the Third Party's employees referred to in Paragraph 1.9.

Part D - Provisions regarding pensions shall not apply.

Appendix 9

Software and EULA

Third Party software (if any) shall be licenced subject to the third party licensor's standard licence terms which shall govern the supply, the Authorities use of and obligations relating to the software in their entirety and which shall prevail in the event of any conflict with the terms and conditions of the Call-Off Contract save for Payment. Third Party Services (if any) shall be supplied subject to the applicable third party's standard service terms. The warranty for Goods shall be as per the applicable third party manufacturer's standard warranty.

Appendix 10

Key Performance Indicators (KPI), Service Level Agreements (SLA), Experience Level Agreements (XLAs), and Reporting Requirements

1. The KPI and SLA which the Parties have agreed shall be used to measure the performance of the Services by the Supplier are contained in the below table.
2. The Supplier is required to manage and provide the Services in such a way as to meet the KPI and SLA.
3. The Supplier shall monitor its performance against each Target KPI and SLA and shall send the Authority a monthly achievement and weekly forecast reports detailing the performance against KPI and SLA in a form and format to be mutually agreed.

The Service Levels Agreements relating to this Contract are as follows: -

#	Service Level Description	Performance Criteria	Target	Event Grading	Credits Applied
1	**Device and Monitor replacement :** Management and resolution of incidents	All Device and Monitor incidents to be resolved within 2 working days of receipt of the Incident (based on Next Working Day delivery of the replacement). Working Days Monday-Friday 08:00-18:00.	48 Hours e.g. an incident assigned at 1pm on a Monday should be closed in the system by 1pm on Wednesday	SLA Level > 98% = **Green status**	No credits
				98% < SLA Level < 97% = **Amber Status**	Four percent (4%) charge of the Monthly Service Charge for that reported Service Period and remediation plan to return service to green;
				97% < SLA Level < 95% = **Red status**	In addition to Four percent (4%) charge of the Monthly Service Charge for that reported Service Period, detailed Remediation Plan; and option for DWP service monitoring;

				95% < SLA Level = **Black status**	In addition to Four percent (4%) charge of the Monthly Service Charge for that reported Service Period, a detailed Remediation Plan, option for DWP service monitoring and Commercial discussion about the future of the service and the remedies available within the Call-Off terms
2	**Repair Cycle and return of devices to stock**	All Devices collected by the supplier from DWP must be in a Functional state and returned to supplier Gold Stock.	Within 30 Calendar Days of Receiving Hardware.	SLA Level > 98% = **Green status**	No credits
				98% < SLA Level < 97% = **Amber Status**	No service credit penalty. Service Improvement Plan in place to return performance achievement to "Green"
				97% < SLA Level < 95% = **Red status**	No service credit penalty. A detailed Remedial Proposal and option for DWP service monitoring
				95% < SLA Level = **Black status**	No service credit penalty. A detailed Remedial Proposal, option for DWP service monitoring and Commercial discussion about the future of the service and the remedies available within the Call-Off terms

3A	**Fulfilment of Standard "Adds" Service Requests**.	All Standard "Adds" Service Requests to be fulfilled within two working days	48 Hours e.g. a request assigned at 1pm on a Monday should be closed in the system by 1pm on Wednesday	SLA Level > 98% = **Green status**	No credits
				98% < SLA Level < 97% = **Amber Status**	Two percent (2%) charge of the Monthly Service Charge for that reported Service Period and remediation plan to return service to green;
				97% < SLA Level < 95% = **Red status**	In addition to Two percent (2%) charge of the Monthly Service Charge for that reported Service Period, a detailed Remedial Proposal, and option for DWP service monitoring;
				95% < SLA Level = **Black status**	In addition to Two percent (2%) charge of the Monthly Service Charge for that reported Service Period, a detailed Remedial Proposal, option for DWP service monitoring and Commercial discussion about the future of the service and the remedies available within the Call-Off terms
3B	**Fulfilment of all Standard "Non Adds" Service Requests**	All Standard "Non Adds" Service Requests to be fulfilled within 5 working days	Five (5) Working Days	SLA Level > 98% = **Green status**	No credits

		Service Requests with the exception of adds must be fulfilled.	e.g. a request assigned at 1pm on a Monday should be closed in the system by 1pm on following Monday.	98% < SLA Level < 97% = **Amber Status**	No service credit penalty. Service Improvement Plan in place to return performance achievement to "Green"
				97% < SLA Level < 95% = **Red status**	No service credit penalty. A detailed Remedial Proposal, and option for DWP service monitoring. Option for Commercial discussion on how to proceed with the service
				95% < SLA Level = **Black status**	No service credit penalty. More detailed Remedial Proposal, option for DWP service monitoring and Commercial discussion about the future of the service and the remedies available within the Call-Off terms
4A	**Asset Management Repository accuracy** Month 1 - Month 3	Asset details for all devices managed by the Supplier, moving in and out of their physical repository, are accurately maintained and are reflected within the DWP Asset repository in DWP Place. Accuracy calculations	98.5% data accuracy	SLA level > 98.5% = **Green status**	No credits. Where accuracy is maintained, periodic audits may be reduced, as agreed between the Parties.
				98.5% < SLA Level < 97.5% = **Amber status**	Three percent (3%) charge of the total Monthly Invoice for that reported Service Period and remediation plan to return service to green;

		against Technow report to be produced on final Friday of each calendar Month. The Supplier will conduct a physical Audit by the end of the Next Working Day, in order to (a) validate accuracy of Technow quantities; and (b) perform all rectification activity, where there exist disparities between the audit and Technow quantities.		97.5% < SLA Level < 95.5% = **Red status**	In addition to Three percent (3%) charge of the total Monthly Invoice for that reported Service Period, detailed Remedial Proposal; and option for DWP service monitoring;
				95.5% < SLA Level = **Black status**	In addition to Three percent (3%) charge of the total Monthly Invoice for that reported Service Period, a detailed Remedial Proposal, option for DWP service monitoring and Commercial discussion about the future of the service and the remedies available within the Call-Off terms
4B	**Asset Management repository accuracy** Month 3 - Month 6	Asset details for all devices managed by the Supplier, moving in and out of their physical repository, are accurately maintained and are reflected within the DWP Asset repository in DWP Place. Accuracy calculations	99% data accuracy	SLA level > 99% = **Green status**	"No credits. Where accuracy is maintained, periodic audits may be reduced, as agreed between the Parties.
				99% < SLA Level < 98% = **Amber status**	Three percent (3%) charge of the total Monthly Invoice for that reported Service Period and remediation plan to return service to green;

		against Technow report to be produced on final Friday of each calendar Month. The Supplier will conduct a physical Audit by the end of the Next Working Day, in order to (a) validate accuracy of Technow quantities; and (b) perform all rectification activity, where there exist disparities between the audit and Technow quantities.		98% < SLA Level < 96% = **Red status**	In addition to Three percent (3%) charge of the total Monthly Invoice for that reported Service Period, detailed Remedial Proposal; and option for DWP service monitoring;
				96% < SLA Level = **Black status**	In addition to Three percent (3%) charge of the total Monthly Invoice for that reported Service Period, a detailed Remedial Proposal, option for DWP service monitoring and Commercial discussion about the future of the service and the remedies available within the Call-Off terms
4C	**Asset Management repository accuracy** Month 6 onwards	Asset details for all devices managed by the Supplier, moving in and out of their physical repository, are accurately maintained and are reflected within the DWP Asset repository in DWP Place. Accuracy calculations	99.5% data accuracy	SLA level > 99.5% = **Green status**	No credits. Where accuracy is maintained, periodic audits may be reduced, as agreed between the Parties.
				99.5% < SLA Level < 98.5% = **Amber status**	Three percent (3%) charge of the total Monthly Invoice for that reported Service Period and remediation plan to return service to green;

		against Technow report to be produced on final Friday of each calendar Month. The Supplier will conduct a physical Audit by the end of the Next Working Day, in order to (a) validate accuracy of Technow quantities; and (b) perform all rectification activity, where there exist disparities between the audit and Technow quantities.		98.5% < SLA Level < 96.5% = **Red status**	In addition to Three percent (3%) charge of the total Monthly Invoice for that reported Service Period, detailed Remedial Proposal; and option for DWP service monitoring;
				96.5% < SLA Level = **Black status**	In addition to Three percent (3%) charge of the total Monthly Invoice for that reported Service Period, a detailed Remedial Proposal, option for DWP service monitoring and Commercial discussion about the future of the service and the remedies available within the Call-Off terms
4D	**(If Integrated)** **Asset Management repository accuracy** Anticipated to be within 6 Months	Asset details for all devices managed by the Supplier, moving in and out of their physical repository, are accurately maintained and are reflected within the DWP Asset repository in DWP Place. Accuracy calculations	100% data accuracy	SLA level = 100% = **Green status**	No credits. Where accuracy is maintained, periodic audits may be reduced, as agreed between the Parties.
				100% < SLA Level < 99% = **Amber status**	Three percent (3%) charge of the total Monthly Invoice for that reported Service Period and remediation plan to return service to green;

		against Technow report to be produced on final Friday of each calendar Month. The Supplier will conduct a physical Audit by the end of the Next Working Day, in order to (a) validate accuracy of Technow quantities; and (b) perform all rectification activity, where there exist disparities between the audit and Technow quantities.		99% < SLA Level < 97% = **Red status**	In addition to Three percent (3%) charge of the total Monthly Invoice for that reported Service Period, detailed Remedial Proposal; and option for DWP service monitoring;
				97% < SLA Level = **Black status**	In addition to Three percent (3%) charge of the total Monthly Invoice for that reported Service Period, a detailed Remedial Proposal, option for DWP service monitoring and Commercial discussion about the future of the service and the remedies available within the Call-Off terms

The Service Levels Reporting requirements relating to this Contract are as follows: -

Service Level Reporting – SLA's					
Title	**Data Source**	**Content**	**Format**	**Frequency**	**Reporting Date**
SLA 1 – Device and Monitor replacement - management and resolution of incidents	DWP Service Now (DWP Place)	All incidents closed in the reporting period, their elapsed time and pass or fail status.	Pass / Fail SLA Attainment % Supporting MI	Monthly	On the first Working Day of every Month

SLA 2 - Repair Cycle and return of devices to stock	Supplier Data Sources	All devices received by the supplier from the authority, Date Received, Date Repaired, repair category, Date returned to Gold Stock, Asset, Serial, model *Any devices that have not been repaired as BER or at Authority request should be marked accordingly.	Pass / Fail SLA Attainment % Supporting MI	Monthly	On the first Working Day of Every Month
SLA 3A – Fulfilment of Standard "Adds" Service Requests	DWP Service Now (DWP Place)	All standard Service Requests Closed within the reporting period for adds, their elapsed time and pass or fail status.	Pass / Fail SLA Attainment % Supporting MI	Monthly	On the first Working Day of Every Month
SLA 3B - Fulfilment of all Standard "Non Adds" Service Requests	DWP Service Now (DWP Place)	All standard Service Requests Closed within the reporting period for move and leavers, their elapsed time and pass or fail status.	Pass / Fail SLA Attainment % Supporting MI	Monthly	On the first Working Day of Every Month
SLA 4A - Asset Management repository accuracy Month 1- Month 6	DWP Service Now (DWP Place) & Supplier audit data	Extract of the supplier stockroom & Output from the supplier audit	Pass / Fail SLA Attainment % Supporting MI	Monthly	On the first Working Day of Every Month
SLA 4B - Asset Management repository accuracy Month 6- Month 12	DWP Service Now (DWP Place) & Supplier audit data	Extract of the supplier stockroom & Output from the supplier audit	Pass / Fail SLA Attainment % Supporting MI	Monthly	On the first Working Day of Every Month

SLA 4C - Asset Management repository accuracy Month 12 onwards	DWP Service Now (DWP Place) & Supplier audit data	Extract of the supplier stockroom & Output from the supplier audit	Pass / Fail SLA Attainment % Supporting MI	Monthly	On the first Working Day of Every Month

The KPIs and KPI reporting requirements relating to this Contract are as follows: -

Title	Data Source	Content	Format	Frequency	Reporting Date
KPI 1 - Aged Incidents	DWP Place (Service Now)	All outstanding incidents at the end of the reporting period, Outstanding Age of each. Overall Average Age of 5 Working Days.	Pass / Fail KPI attainment 98.5% Supporting MI	Monthly	On the first Working Day of Every Month
KPI 2 – Aged Service Requests	DWP Place (Service now)	All outstanding standard Service Requests at the end of the reporting period, Outstanding Age of each. Overall Average Age of 10 Working Days.	Pass / Fail KPI attainment 95% Supporting MI	Monthly	On the first Working Day of Every Month

KPI 3 – NSSR quotes and accuracy	DWP Place (Service Now) * Supplier Data	3a Provide a response including a quote and delivery timescales to NSSR within 3 working days.	Pass / Fail KPI attainment 98% Supporting MI	Monthly	On the first Working Day of Every Month
		3b All NSSRs completed and Invoiced in the Period. Comparison of actual price and timescale for completion with original quote and delivery timescale.	Pass / Fail KPI attainment 98% within 10% of quote Supporting MI	Monthly	On the first Working Day of Every Month
KPI 4 – Project request quotes and accuracy	DWP Place (Service Now) * Supplier Data	Provide a response including a quote and delivery timescales to Project Request within 15 working days	Pass / Fail KPI attainment 90% Supporting MI	Monthly	On the first Working Day of Every Month

KPI 5a – Asset Management Updates	DWP Place. DWP sample check	Following movement of devices in and out of the Supplier stockroom changes to Asset records in the DWP Asset Repository are completed within 48 hours	Pass / Fail KPI attainment 99.5% Supporting MI	Weekly	On the first Monday (or where a Public Holiday, next Working Day) of every week
KPI 5b – Asset Management corrections	DWP Place. DWP sample check	Throughout the service period the Supplier to check the accuracy of the Asset record changes made and correct 99.5% of errors within 48 hours This will be validated by DWP sample checking	Pass / Fail KPI attainment 99.5% Supporting MI	Weekly	On the first Monday (or where a Public Holiday, next Working Day) of every week
KPI 6 – Invoicing Accuracy	Supplier invoicing	All invoices submitted within required timescales	Pass / Fail KPI attainment 99.5%	Monthly	On the first Working Day of Every Month

		All invoices presented against the correct Purchase Order references	Supporting MI		
		All invoices raised for the correct amount			
		Any discrepancies resolved within required timescales			

The Experience Level Agreements (XLA) relating to this Contract are as follows: -

Device and Monitor Replacement Service				
XLA	**I had a positive experience with the Supplier**	**Ratings**		
XI - 1	Contact to arrange my replacement was professional, polite and courteous	Exceeded Expectations	As Expected	Below Expectations
XI - 2	My replacement was delivered within the agreed expectations	Exceeded Expectations	As Expected	Below Expectations
XI - 3	The delivery engineer was professional, polite and courteous	Exceeded Expectations	As Expected	Below Expectations
Standard Service Requests				

XLA	I had a positive experience with the Supplier	Ratings		
XI - 1	Contact to arrange fulfilment of my request was professional, polite and courteous	Exceeded Expectations	As Expected	Below Expectations
XI - 2	My request was completed within the agreed expectations	Exceeded Expectations	As Expected	Below Expectations
XI - 3	The engineer was professional, polite and courteous	Exceeded Expectations	As Expected	Below Expectations

Note: Scoring and measurement criteria to be agreed upon Service Transition. Meeting the XLA in the reporting period may be used to offset any financial penalties against any potential corresponding SLA failures. This will be at the discretion of the Authority.

The XLA Reporting Requirements relating to this Contract are as follows: -

XLA Reporting				
Title	**Data Source**	**Content**	**Format**	**Frequency**
XLA 1 – Device and Monitor Replacement Service “I had a positive experience with the Supplier”	To be agreed at Service Transition	Supporting XI outputs	To be agreed at Service Transition	Monthly
XLA 2 – Standard Service Request “I had a positive experience with the Supplier”	To be agreed at Service Transition	Supporting XI outputs	To be agreed at Service Transition	Monthly

Additional Reporting Requirements relating to this Contract are as follows: -

Additional Reporting Requirements				
Title	**Data Source**	**Content**	**Format**	**Frequency**
BER (Beyond Economical Repair)	Supplier Source Data	All devices received and assessed that have been deemed BER by the supplier. Asset, Serial, Make, Model and reason these are proposed as BER	Summary of volumes based on make and model with backing data	Monthly
Disposal	Supplier Source Data	All devices disposed of within the reporting period. Report to include Asset, Serial, Make, Model, Date of Disposal, Confirmation WEE certificate has been sent to the Authority, date provided	Summary of volumes based on make and model with backing data	Monthly
Re-Sale	Supplier Source Data	All devices proposed for resale within the reporting period. Report to include Asset, Serial, Make, Model, Value	Summary of Value against make and model, with backing data	Monthly
Continual Service Improvement (CSI) initiatives	N/A	Minimum of x2 tangible CSI Initiatives To include: description, benefits, category, any indicative costs (if applicable	Presentation at Monthly Service Review	Quarterly

Stockholding – Historical demand	DWP Service Now (DWP Place) & Supplier source data	Volume of Devices provisioned against Incidents & Standard, NSSR and Project requests, by make and model.	3 Month rolling view of historical device and Monitor provision against Core Services. By Month.	Monthly
Stockholding – Stock Status	Supplier Data Source (to move to DWP Service Now where possible)	High Level Volume report of all stock held and its availability status. E.g. ready to deploy, In repair	Stock status by Make/Model	Weekly
Repairs	Supplier Data Source	volume of devices & monitors entering the repair loop, the outcome of the assessment, warranty status, pricing and repair status	Summary of volume of repairs against make and model, warranty and repair status	Monthly
Trend Analysis	DWP Service Now (DWP Place) & Supplier source data	Any significant trends in incident types based on Tech Now or Repair data. Volume of issues by trend	Trend identified & associated volumes	Quarterly
Obligation Management	Contractual Obligations	A full list of all contractual obligations, Met/Not Met, evidence on how these are being met or mitigated if they are not	Total Number of obligations / Volume of Pass/ Fail and overall % compliant	Quarterly
Security Incidents	Supplier Data	Any security incidents identified by the supplier that has or could cause any physical or reputational damage to the Authority	Description of issue, latest status, impact	Monthly

Aged debt and open invoices	Supplier Source Data	Any invoices not yet paid including details of : Invoice reference, PO reference, Value, Due date Days overdue (if applicable)	Presented at Monthly Commercial & Operational Board	Monthly
Contract Spend	Supplier Source Data	Spend to date against the contract, split by service line/purchase order	Presented at Monthly Commercial & Operational Board	Monthly

1. SLA Calculations

1.1. Asset Management Repository assessed under SLA 4 shall be calculated by using the following calculation:

Calculation: Devices handled by Supplier in service period = A Devices updated correctly = B Calculation of accuracy = B/A*100

1.2. The Supplier shall adhere to these principles for the purposes of Asset Management Repository calculation

1.2.1. A report will be provided of devices handled within the service period including:

(a) Devices held by Supplier (previous months baseline);

(b) Devices moved in to Supplier Stock (with relevant incident or request references);

(c) Devices moved out of Supplier Stock (with relevant incident or request references);

(d) Devices left in Supplier Stock (new baseline)

1.2.2. The report will provide Serial Numbers consistent with the DWP Place asset repository.

1.2.3. The total number of Devices (1) includes any 'computer' device handled within the calendar month by the Supplier e.g. Laptops, 2 in1's, Mini-PC's and Desktops

1.2.4. The total number of errors linked to the asset record for a device handled by the Supplier. This could be related to one issue or a combination of issues related to the following: (the device is only counted once even if there is more than one error):

(a) Asset Tag

(b) Serial number

(c) Location

(d) Stat

(e) Sub-state

(f) Model

(g) Stockroom

(h) Any other asset information in the TechNow asset repository relevant to the service provided by the Supplier.

2. Monitoring SLA Performance

2.1. Performance by the Supplier against each SLA shall be graded as follows:

SLA Status	Description
Green	Meets the SLA
Amber	Some failure to meet the SLA which requires a remediation plan for corrective action.
Red	Material failure to meet the SLA which requires a remediation plan and allows options for service monitoring
Black	Significant failure to meet the SLA which requires a remediation plan, allows options for service monitoring and

	Commercial discussion about the future of the service and the remedies available within the Call-Off terms

2.2. Service Credits shall be applied as described in the Credits Applied section in Section IV. A maximum monthly Service Credit Cap of nine percent (9%) of the Monthly Service Charge for a reported Service Period shall be applied throughout the term of the Call-off Contract.

2.3. Performance management will be monitored according to the governance framework within this Call-Off agreement (Appendix 17). The detail will be agreed during Implementation and documented in the Operations Manual

3. Service Level Multiple Failure Event

3.1. A Service Level Multiple Failure event shall occur where 3 consecutive months where 1 or more SLA fails, which may result in Commercial discussions about the future of the service and the remedies available within the Call-Off terms

4. Service remediation

4.1 If there is a Service Level Failure, the Supplier shall:

4.1.1. notify the Authority immediately of the Service Level Failure;

4.1.2. provide the Authority with a draft remediation plan which sets out the steps to be taken by the Supplier in order to remedy the Service Level Failure and prevent recurrence;

4.1.3. deploy all additional resources and take all remedial action that is necessary to rectify or to prevent the Service Level Failure from recurring; and

4.1.4. carry out the actions identified in remediation Plan in accordance with its terms, at the Suppliers cost.

4.2. Other than in the following circumstances:

4.2.1. Any negligent act or omission of the Authority;

4.2.2. Any breach of an express provision of this Contract by the Authority;

4.2.3. Any Force Majeure Event;

For the purposes of this agreement, Relief Event means

(i) any breach of any express provision of this Contract by the Authority including without limitation an obligation to comply with the Authority's obligations which is a direct cause of the SLA failure;

(ii) any negligent act or omission of the Authority which is a direct cause of the SLA failure; and/or

(iii) any Force Majeure Event.

Appendix 11

Subcontractor Information

Cameo - Break-fix of Microsoft Surface devices
Tier 1 - Disposal of Assets
Rico Logistics - Secure Courier

Appendix 12

DWP Additional Clauses

Not Used in this Contract.

Appendix 13

DWP Security Schedule

1. GENERAL

The Supplier shall, and shall procure that any Sub-Contractor (as applicable) shall, comply with the Authority's security requirements as set out in the Contract which include the requirements set out in this Appendix 13 to the Contract (the "**Authority's Security Requirements**"). The Authority's Security Requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Authority Assets, the Authority's Systems Environment and the Supplier's Systems Environment.

2. PRINCIPLES OF SECURITY

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

3. ISO/IEC 27001 COMPLIANCE AND AUDIT

3.1 The Supplier shall, and shall procure that any Sub-Contractor (as applicable) shall, comply with ISO/IEC 27001 in relation to the Services during the Contract Period.

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

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

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

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

c) a statement of applicability;

d) a risk treatment plan; and

e) an incident management plan

in each case as specified by ISO/IEC 27001.

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

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

3.6 Notwithstanding the provisions of paragraph 3.1 to paragraph 3.4, the Authority may, in its absolute discretion, notify the Supplier that it is not in compliance with the Authority′s Security Requirements and provide details of such non-compliance. The Supplier shall, at its own expense, undertake those actions required in order to comply with the Authority′s Security Requirements within one calendar month following such notification or on a date as agreed by the Parties. For the avoidance of doubt, any failure to comply with the Authority′s Security Requirements within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a Material Breach.

4. CYBER ESSENTIALS SCHEME

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

4.2 The Supplier shall notify the Authority of any failure to obtain, or the revocation of, a Cyber Essentials Certificate within 2 Working Days of confirmation of such failure or revocation. The Supplier shall, at its own

expense, undertake those actions required in order to obtain a Cyber Essentials Certificate following such failure or revocation. For the avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Certificate during the Contract Period after the first date on which the Supplier was required to provide a Cyber Essentials Certificate in accordance with paragraph 4.1 (regardless of whether such failure is capable of remedy) shall constitute a Material Breach.

5. RISK MANAGEMENT

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

5.2 The Supplier shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Supplier′s Systems Environment or in the threat landscape or (iii) at the request of the Authority. The Supplier shall provide the report of the Risk Assessment to the Authority, in the case of at least annual Risk Assessments, within 5 Working Days of completion of the Risk Assessment or, in the case of all other Risk Assessments, within one calendar month after completion of the Risk Assessment or on a date as agreed by the Parties. The Supplier shall notify the Authority within 5 Working Days if the Risk Profile in relation to the Services has changed materially, for example, but not limited to, from one risk rating to another risk rating.

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

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

5.5 For the avoidance of doubt, the Supplier shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this paragraph 5. Any failure by the Supplier to comply with any requirement of this paragraph 5 regardless of whether such failure is capable of remedy, shall constitute a Material Breach.

6. SECURITY AUDIT AND ASSURANCE

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

6.2 The Supplier shall conduct Security Tests to assess the Information Security of the Supplier′s Systems Environment and, if requested, the Authority′s Systems Environment. In relation to such Security Tests, the Supplier shall appoint a third party which i) in respect of any Penetration Test, is duly accredited by CHECK, CREST (International), or Tigerscheme and, ii) in respect of any Security Test to which PCI DSS apply, is an approved scanning vendor duly accredited by the PCI. Such Security Test shall be carried out (i) at least annually, (ii) in the event of a material change in the Supplier′s Systems Environment or in the Authority′s System Environment or (iii) at the request of the Authority which request may include, but is not limited to, a repeat of a previous Security Test. The content, and format of any report of such Security Tests shall be approved in advance of the Security Test by the Authority. The Supplier shall provide any report of such Security Tests within one calendar month following the completion of such Security Test or on a date agreed by the Parties. The Supplier shall, at its own expense, undertake those actions required to rectify any risks identified by any Security Test in the manner and within the timeframe required by the Authority in its absolute discretion.

6.3 The Authority shall be entitled to send the Authority′s Representative to witness the conduct of any Security Test. The Supplier shall provide to the

Authority notice of any Security Test at least one month prior to the relevant Security Test.

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

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

7. SECURITY POLICIES AND STANDARDS

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

7.2 Notwithstanding the foregoing, the Authority′s Security Requirements applicable to the Services may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the Services. Where any such change constitutes a Contract Change, any change in the Authority′s Security Requirements resulting from such Contract Change (if any) shall be agreed by the Parties in accordance with the Contract Change Procedure. Where any such change constitutes an Operational Change, any change in the Authority′s Security Requirements resulting from such Operational Change (if any) shall be agreed by the Parties and documented in the relevant Operational Change Confirmation.

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

ANNEX A – 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/publications/hmg-personnel-security-controls)

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

ANNEX B – SECURITY STANDARDS

The Security Standards are published on:

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

bb) SS-033 - Patching

Appendix 14

DWP GDPR Clauses

Appendix 14, Part A

PROTECTION OF INFORMATION

1. Authority Data

1.1 The Supplier shall not delete or remove any proprietary notices contained within or relating to the Authority Data.

1.2 The Supplier shall not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Supplier of its obligations under this Contract or as otherwise expressly authorised in writing by the Authority.

1.3 To the extent that Authority Data is held and/or processed by the Supplier, the Supplier shall supply that Authority Data to the Authority as requested.

1.4 The Supplier shall take responsibility for preserving the integrity of Authority Data and preventing the corruption or loss of that data.

1.5 The Supplier shall perform secure back-ups of all Authority Data and shall ensure that up-to-date back-ups are stored off-site in accordance with the Business Continuity Plan. The Supplier shall ensure that such back-ups are available to the Authority at all times upon request. Confirmation that secure back-ups have been performed in accordance with the Authority's requirements as specified in this clause 1.5 shall be provided to the Authority no less than every three (3) Months.

1.6 The Supplier shall ensure that any system or media on which the Supplier holds any Authority Data, including back-up data, is a secure system that complies with the Security Policies and Standards.

1.7 If the Authority Data is corrupted, lost or sufficiently degraded as a result of the Supplier's Default so as to be unusable, the Authority may:-

a) require the Supplier (at the Supplier's expense) to restore or provide for the restoration of the Authority Data and the Supplier shall do so as soon as practicable but not later than [ten (10) days]; and/or;

b) itself restore or provide for the restoration of the Authority Data and shall be repaid by the Supplier any reasonable expenses incurred in doing so.

1.8 If at any time the Supplier suspects or has reason to believe that the Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Supplier shall notify the Authority immediately and inform the Authority of the remedial action the Supplier proposes to take.

1.9 The Supplier 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 Supplier 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 1.9 shall apply to Landed Resources.

1.10 Where the Authority has given its prior written consent to the Supplier to access, process, host or transfer Authority Data from premises outside the United Kingdom (in accordance with clause 1.9 of the Contract):-

a) the Supplier 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 Supplier 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 any applicable exception or exemption.

1.11 Any breach by the Supplier of clause 1 shall be a Material Breach.

1.12 In the event the Supplier goes into Liquidation or the Contract is terminated by the Authority pursuant to the provisions of the Contract relating to termination on insolvency, the Supplier (or a liquidator or provisional liquidator acting on behalf of the Supplier) shall at its own cost and at no cost to the Authority:-

a) conduct a full and thorough search for any electronic and paper records held by the Supplier which contain Authority Data/Information/Information [relating to a Authority/service user]; in accordance with the Authority instructions;

b) return all such records as described in clause 1.12(a) to the Authority in accordance with their instructions;

c) permanently destroy all copies of any relevant electronic records; and

d) provide written confirmation to the Authority that the actions outlined above in this clause have been completed.

1.13 In the event of a Sub-contractor being in then it is the responsibility of the Supplier to recover records held by the Sub-contractor and provide assurance to the Authority that they have been recovered.

1.14 In the event the Supplier is put into Administration the Authority will work closely with the administrator to ensure the Supplier is able to maintain Authority and other records they have created and held in accordance with this clause 1 of this Contract and maintain these standards in the safekeeping of Authority information, i.e. these records must be stored in accordance with Authority information assurance and HMG Cabinet Office information security standards.

2 Protection of Personal Data (Authority is Data Controller)

2.1 Each of the Parties including the personnel of each Party (personnel shall include directors, officers, employees, servants, agents, consultants, suppliers and sub-contractors) will comply with all of its applicable requirements of the Data Protection Legislation and shall not knowingly or negligently by any act or omission, place the other Party in breach, or potential breach of Data Protection Legislation. This clause is in addition to and does not relieve, remove or replace a Party's obligations under the Data Protection Legislation.

2.1B The Authority shall be the Data Controller of the information listed in Part B Annex B Part 1.

2.2 With respect to the Parties rights and obligations under the Contract, the Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Data Controller and the Supplier is the Data Processor unless otherwise specified in Part B.

2.3 The Supplier shall notify the Authority immediately if it considers that any of the Authority's instructions infringe the Data Protection Legislation.

2.4 The Supplier shall provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Authority, include (without limitation):-

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

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

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.

2.5 The Supplier shall, in relation to any Personal Data processed or to be processed in connection with its obligations under this Contract:-

a) process that Personal Data only to the extent and in such manner as is necessary for the purposes specified in this Contract and in accordance with Part B, unless the Supplier is required to process the Personal Data otherwise by Law. In such case, the Supplier shall inform the Authority of that legal requirement unless the Law prevents such disclosure on the grounds of public interest;

b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Data Controller may reasonably reject (but failure to reject shall not amount to approval by the Data Controller of the adequacy of the Protective Measures) having taken account of the:-

(i) nature of the Personal Data to be protected;

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

(iii) state of technological development; and

implement any Protective Measures at the Supplier′s own expense and at no cost to the Authority;

c) ensure that it and its Staff:-

(i) do not process Personal Data except in accordance with this Contract and Data Protection Legislation and access to such data is limited to those Staff who need to access Personal Data to meet the Supplier′s Data Processor duties under the Contract and Data Protection Legislation

(ii) and only collect Personal Data on behalf of the Authority in the format agreed with the Authority which shall contain a data protection notice informing the Data Subject of the identity of the

Data Controller, the identity of any data protection representative it may have appointed, the purpose(s) for which the Data Subject's Personal Data will be processed and any other information, which is necessary to comply with Data Protection Legislation. The Supplier shall not modify the format agreed with the Authority without the prior written consent of the Authority;

(iii) take all reasonable steps to ensure the reliability and integrity of any Staff who have access to the Personal Data and ensure that they:-

(A) are aware of and comply with the Supplier's duties under clause 2;

(B) are subject to appropriate confidentiality undertakings including between the Supplier and any Sub-processor;

(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 Authority or as otherwise permitted by this Contract or required to do so under a legal requirement/court order (provided that the Supplier shall give notice to the Authority of any disclosure of Personal Data that it or any of its Staff is required to make under such a legal requirement or court order immediately when it is made aware of such a requirement); and

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

d) not transfer Personal Data outside of the European Economic Area or International Organisation unless the prior written consent of the Authority has been obtained and provided the following conditions are fulfilled:-

(i) the Authority or the Supplier 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;

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

(iii) the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

(iv) the Supplier complies with any reasonable instructions notified to it in advance by the Authority with respect to the processing of the Personal Data.

e) at the written direction of the Authority, delete or return Personal Data (and any copies of it) using a secure method of transfer to the Authority on expiry or earlier termination of the Contract unless the Supplier is required by Law to retain the Personal Data;

f) permit the Authority or the Authority′s designated representative or external auditors to inspect and audit the Supplier′s Data Processor activities (and/or those of its Staff) and comply with all reasonable requests or directions by the Authority to enable the Authority to verify that the Supplier is in full compliance with its obligations under the Contract.

2.6 Subject to clause 2.7, the Supplier shall notify the Authority immediately if it:-

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

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

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

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

e) 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

f) becomes aware of a Data Loss Event.

2.7 The Supplier′s obligation to notify the Authority under clause 2.6 shall include the provision of further information to the Authority as soon as reasonably practicable as details become available.

2.8 Taking into account the nature of the processing, the Supplier shall provide the Authority with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request

made under clause 2.6 (and insofar as possible within the timescales reasonably required by the Authority) at no cost to the Authority including by promptly providing:-

a) the Authority with full details and copies of the complaint, communication or request;

b) such assistance as is reasonably requested by the Authority to enable the Authority to comply with a Data Subject Request promptly and in any event within the relevant timescales set out in the Data Protection Legislation;

c) the Authority, at its request, with any Personal Data it holds in relation to a Data Subject;

d) assistance as requested by the Authority following any Data Loss Event including but not limited to such assistance to enable the Authority to mitigate the impact of the Data Loss Event, to ensure that a Data Loss Event of the same nature does not occur again, to notify the competent regulatory body of the Data Loss Event and/or to notify the Data Subjects of the Data Loss Event;

e) assistance as requested by the Authority with respect to any request from the Information Commissioner′s Office, or any consultation by the Authority with the Information Commissioner's Office.

2.9 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with its Data Processor obligations under this clause 2. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:-

a) the Authority determines the processing is not occasional;

b) the Authority determines the processing includes any Special Categories of Personal Data and/or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

c) the Authority determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

2.10 The Supplier shall keep a record of any processing of Personal Data it carries out on behalf of the Authority including (without limitation) the records specified in Article 30(2) of the GDPR and upon request provide a copy of the record of the processing of any Personal Data it carries out on behalf of the Authority including (without limitation) the records specified in Article 30(2) of the GDPR.

2.11 The Supplier shall designate its own Data Protection Officer if required by Data Protection Legislation or by the Authority in writing.

2.12 Before allowing any Sub-processor to process any Personal Data under this Contract, the Supplier must:-

a) notify the Authority in writing of the intended Sub-processor and processing;

b) obtain the advance written consent of the Authority to allow the Sub-processor to process any Personal Data under the Contract;

c) enter into a written contract with the Sub-processor which reflects the terms set out in this clause 2 such that they apply to the Sub-Processor as a Data Processor; and

d) provide the Authority with such information regarding the Sub-processor as the Authority may reasonable require.

2.13 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor and/or Staff.

2.14 The Authority may, at any time on not less than thirty (30) Working Days advance notice, revise this clause by replacing it with any applicable Data Controller/Data Processor standard clauses or similar terms forming part of an applicable certification scheme under the Data Protection Legislation (which shall apply when incorporated by an attachment to this Contract).

2.15 The Supplier shall comply with guidance issued by the Information Commissioner′s Office. The Authority may on not less than thirty (30) Working Days notice to the Supplier amend this Contract to ensure that it complies with any guidance issued by the Information Commissioners Officer and/or any changes to Data Protection Legislation.

2.16 The Supplier shall indemnify and keep the Authority indemnified in full from and against all claims, proceedings, actions, damages, loss, penalties, fines, levies, costs and expenses and all loss of profits, business revenue or goodwill (whether direct or indirect) and all consequential or indirect loss howsoever arising out of, in respect of or in connection with, any breach by the Supplier or any of its Staff of this clause 2.

Appendix 14, Part B – PERSONAL DATA AND DATA SUBJECTS

ANNEX A – DATA PROCESSING

1. The Data Processor shall comply with any further written instructions with respect to processing by the Data Controller.

2. Any such further instructions shall be incorporated into this Part B Annex A.

3. This Part B Annex A shall be completed by the Data Controller, who may take account of the view of the Data Processor, however the final decision as to the content of this Part B Annex A shall be with the Data Controller at its absolute discretion

4. The contact details of the Data Processor's Data Protection Officer are Cara Dearman, Senior Privacy Counsel, cara.dearman@cdw.com

Description	Details
Identify of: the Data Controller the Data Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Data Controller (DATA.PROTECTION@DWP.GOV.UK) and the Supplier is the Data Processor in accordance with clause 2.2
Subject matter of the processing	Device Support & Request Services Contract
Duration of the processing	24 months

Nature and purposes of the processing	User home address and phone number to facilitate home deliveries and device swaps
Type of Personal Data	Home address, mobile phone number
Categories of Data Subject	Official – containing personal data
Plan for return and destruction of the data once the processing is complete UNLESS requirement under European Union or European member state law to preserve that type of data	Data to be deleted at end of contract term where possible

ANNEX B – DATA CONTROLLER

PART 1

The Authority shall be the Data Controller of:

Employee personal data

PART 2

The Controller shall be the Data Controller of:

Employee personal data

Appendix 15

Data Protection Protocol

Not used in this Contract.

Appendix 16

Information Security Questionnaire

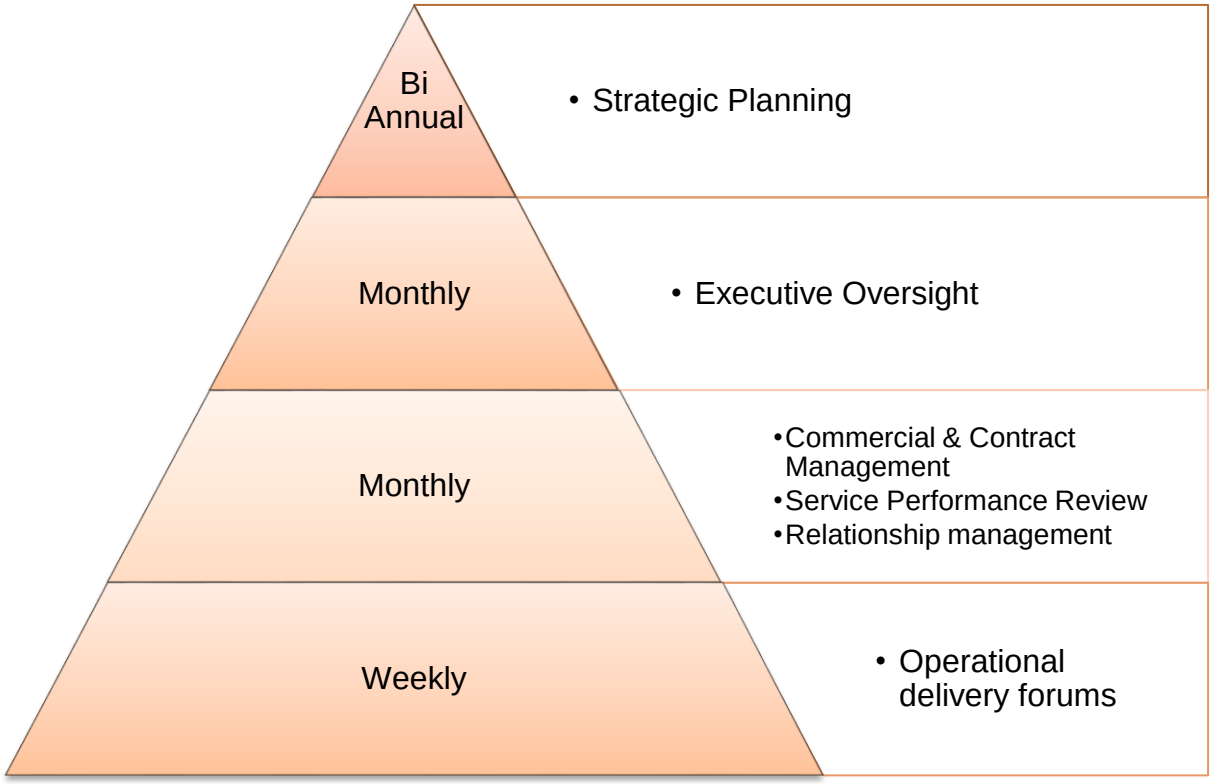
Device Services
Information Security (

Included in Addendum 6

Appendix 17

GOVERNANCE

1. The Parties shall apply the following Board structures and representations for the performance monitoring of this agreement, the detail of which shall be held in the Operations Manual.



Appendix 18

DWP Invoicing Policy

1. The Supplier agrees to the following policies regarding invoicing:

1.1. The Supplier must provide accurate invoices and supporting Management Information on a monthly basis.

1.2. The Authority shall create a Purchase Order (PO) per service line which the Supplier must invoice accurately against. In the case of the Supplier invoicing against the incorrect Purchase Order, the Authority will reject the invoice.

1.3. The Supplier shall ensure that any invoice or credit note includes, without limitation, the following information:

1.3.1.The Purchase Order reference

1.3.2.The date of the invoice

1.3.3.A unique, numerical invoice number

1.3.4.The period to which the charges relate

1.3.5.Details of the correct contract reference

1.3.6.A contact name and telephone number of a responsible person in the Supplier's Finance department in the event of any administrative queries

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

1.3.8.Clear indication of whether it is a credit note or invoice

1.3.8.1.In the case of a credit note, detail of the invoice number the credit note is being raised against

1.3.9.The amounts charged, broken down at a summary level and matching the amounts detailed in the Management Information outlined in 1.5

1.4. Where any invoice or credit note does not conform to the Authority's requirements detailed in 1.3 and therefore does not constitute a valid invoice or credit note, the Authority will reject this invoice or credit note.

1.5. Any invoice or credit note shall be accompanied with Management Information (MI), the format and content of which shall be agreed during the on-boarding process. This MI shall include, without limitation, the following information:

1.5.1.The dates upon which the services being charged were performed

1.5.2.Detail of the services being charged including volumes and unit costs

1.5.3.The methodology applied to calculate the charges

1.5.4.The invoice and Purchase Order reference that the MI corresponds to

1.6. The Supplier shall submit, as soon as possible and in any case within ten (10) Working Days after the end of each calendar month, all invoices and accompanying Management Information in such format as the Authority may specify from time to time, for the Charges incurred during that calendar month.

1.6.1. Invoices and credit notes shall be submitted to:

APinvoices-DWP-U@gov.sscl.com

workplace.computing@invoices.dwp.gov.uk

1.6.2. With all supporting documentation and management information also submitted to:

workplace.computing@invoices.dwp.gov.uk

1.7. At the point that the Authority notes a discrepancy in the billing, the Supplier shall respond within 3 working days with agreement or with further clarification. Discrepancies must be settled by the Supplier in the form of a credit note within 3 working days of such agreement. If this credit note is not raised within 10 working days of such agreement, the Authority may reject the invoice and ask the Supplier to re-invoice for the correct amount.

1.8. The Authority shall have 6 months in which to raise any billing discrepancies. Any discrepancies raised after this point shall not be liable for remedy by the Supplier. For the avoidance of doubt, this 6-month deadline shall only apply where the Supplier has responded to invoicing queries within the agreed timescales outlined in 1.7.

1.9. The Supplier must provide any invoices to the Authority within 6 months of the completion of delivery of the relevant Services to which the invoice relates. Invoices delivered after expiry of this period shall be invalid and the Authority shall have no liability in respect of such invoices.

Appendix 19

DEFINITIONS AND INTERPRETATION

1. In this Contract the following words shall have the following meanings unless the context requires otherwise:

"**Actual Services Commencement Date"**	means the date the Supplier actually commences delivery of all of the Services;
"**Administration"**	means the administrative receivership of a company under the management of an administrator under the Insolvency Act 1986 (as amended).
"Affiliate"	means in relation to any company, any holding company or subsidiary of that company or any subsidiary of such holding company, and "holding company" and "subsidiary" shall have the meaning given to them in section 1159 of the Companies Act 2006
"**Asset Management Repository"**	DWP Hardware Asset Management Repository within DWP Place (DWP Service Now), where all Hardware Assets are recorded and tracked using their asset details and supporting information, including; Serial Number, Device Hostname, Asset Tag, Make, Model, Assigned User, installation date, Location, Stockroom and State, so assets can be tracked from procurement, throughout the asset lifecycle until disposal (end of life)
"**Authority Assets"**	means any Authority Devices and Authority Data;

"Authority Cause"	means any breach by the Authority of the Authority's Obligations and obligations under the call off terms that is the result of any act, omission or negligence by the Authority or where Supplier is delayed from discharging an obligation under the Contract due to an Authority act, omission or negligence.
"Authority Data"	means the data, guidance, specifications, instructions, toolkits, plans, databases, patents, patterns, models, design, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:- (i) supplied to the Supplier by or on behalf of the Authority; or (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract.
"Authority Personnel"	shall mean all persons employed by the Authority including directors, officers, employees together with the Authority's servants, agents, consultants, Suppliers and suppliers but excluding the Supplier and any Sub-Contractor (as applicable).
"**Authority's Obligations"**	means the Authority's further obligations, if any, referred to in the Specification and Tender Response Document and/or the Order Form;

"**Authority's Representative"**	means the person representing the Authority that signs this Call-off Contract.
"**Authority's Security Requirements"**	means the Authority's security requirements set out in the Contract which include the requirements set out in Schedule [6] to the Contract.
"**Authority's Systems Environment"**	means all of the Authority's ICT systems which are or may be used for the provision of the Services.
"**Authority"**	means the authority named on the Order Form;
"Availability Test"	shall mean the activities performed by the Supplier to confirm the availability of any or all components of any relevant ICT system as specified by the Authority.
"**Breach Notice"**	means a written notice of breach given by one Party to the other, notifying the Party receiving the notice of its breach of this Contract;

"**Breach of Security"**	means the occurrence of: (i) any unauthorised access to or use of Authority Assets, the Authority's Systems Environment (or any part thereof) and Supplier's Systems Environment (or any part thereof); (ii) the loss and/or unauthorised disclosure of any Authority Assets, the Authority's Systems Environment (or any part thereof) and Supplier's Systems Environment (or any part thereof); (iii) any unauthorised event resulting in loss of availability of any Authority Assets, Authority's Systems Environment (or any part thereof) and Supplier's Systems Environment (or any part thereof); (iv) any unauthorised changes or modification to any Authority Assets, the Authority's Systems Environment (or any part thereof) and Supplier's Systems Environment (or any part thereof).

"**Bribery Act 2010"**	means the Bribery Act 2010 and any subordinate legislation made under that Act from time to time together with any guidance or codes of practice issued by the relevant government department concerning the legislation.
"**Business Continuity Event"**	means any event or issue that could impact on the operations of the Supplier and its ability to supply the Goods and/or provide the Services including an influenza pandemic and any Force Majeure Event;
"**Business Continuity Plan"**	means the Supplier's business continuity plan which includes its plans for continuity of the supply of the Goods and the provision of the Services during a Business Continuity Event;
"**Business Day"**	means any day other than Saturday, Sunday, Christmas Day, Good Friday or a statutory bank holiday in England and Wales;
"**Cabinet Office Statement"**	the Cabinet Office Statement of Practice – Staff Transfers in the Public Sector 2000 (as revised 2013) as may be amended or replaced;

"**Call-off Contract Charges"**	means the prices (inclusive of any Milestone Payments and exclusive of any applicable VAT), payable to the Supplier by the Authority under this Call Off Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under this Call Off Contract less any Deductions;
"**Call-off Terms and Conditions"**	means these Call-off Terms and Conditions for the Supply of Goods and the Provision of Services;
"Call Off Guarantee"	means a deed of guarantee that may be required under this Call Off Contract in favour of the Authority.
"Call Off Guarantor"	means the person in the event that a Call Off Guarantee is required under this Call Off Contract acceptable to the Authority to give a Call Off Guarantee;
"**Change Control Process"**	means the change control process defined under Section 42 of Appendix A Call-off Terms and Conditions
"CHECK"	shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.
"Cloud"	shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data.

“CloudFirst Device”	refers to an Authority Desktop Device or Laptop Device managed and maintained by InTune MDM and built via AutoPilot
“**Codes of Practice”**	shall have the meaning given to the term in Clause 1.2 of Schedule 3 of Appendix A Call-off Terms and Conditions;
“**Commencement Date”**	means the date the Authority Representative signs thisCall-Off agreement;
“**Confidential Information”**	means information, data and material of any nature, which either Party may receive or obtain in connection with the conclusion and/or operation of the Contract including any procurement process which is: (a) Personal Data including without limitation which relates to any patient or other service user or his or her treatment or clinical or care history; (b) designated as confidential by either party or that ought reasonably to be considered as confidential (however it is conveyed or on whatever media it is stored); and/or (c) Policies and such other documents which the Supplier may obtain or have access to through the Authority’s intranet;
“**Contract Manager”**	means for the Authority and for the Supplier the individuals specified in the Call-Off agreement or as otherwise agreed between the Parties in writing or such other person notified by a Party to the other Party from time to time in accordance with Clause 8.1 of Schedule 2 of Appendix A Call-off Terms and Conditions;

"**Contract Price"**	means the price exclusive of VAT that is payable to the Supplier by the Authority under the Contract for the full and proper performance by the Supplier of its obligations under the Contract calculated in accordance with the provisions of the Framework Agreement and as confirmed in the Order Form;
"**Contract"**	means the Order Form, the provisions on the front page of Appendix A and all Schedules of Appendix A Call-off Terms and Conditions, the Specification and Tender Response Document and the applicable provisions of the Framework Agreement;
"**Contracting Authority"**	means any contracting authority as defined in Regulation 3 of the Public Contracts Regulations 2015 (SI 2015/102) (as amended), other than the Authority;
"**Controller"**	shall have the same meaning as set out in the GDPR;
"**Convictions"**	means, other than in relation to minor road traffic offences, any previous or pending prosecutions, convictions, cautions and binding-over orders (including any spent convictions as contemplated by Section 1(1) of the Rehabilitation of Offenders Act 1974 or any replacement or amendment to that Act);
"Cyber Essentials"	shall mean the Government-backed, industry-supported scheme managed by the NCSC to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.

"Cyber Security Information Sharing Partnership" or "CiSP"	shall mean the cyber security information sharing partnership established by the NCSC or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
"**Data Protection Legislation"**	means (i) the Data Protection Act 1998 or, from the date it comes into force, the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; (ii) the GDPR, the Law Enforcement Directive (Directive (EU) 2016/680) and any applicable national implementing Law as amended from time to time; and (iii) all applicable Law about the processing of personal data and privacy;
"**Data Protection Officer"**	shall have the same meaning as given in Data Protection Legislation.
"**Data Protection Protocol"**	means any document of that name as provided to the Supplier by the Authority (as amended from time to time in accordance with its terms) which shall include, without limitation, any such document appended to the Order Form;
"**Data Subject Request"**	means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation.
"Data Subject"	shall have the same meaning as given in Data Protection Legislation.

“Dead on Arrival (DOA)”	refers to a Device that, at the point of delivery from the Supplier, is either physically damaged or when turned on does not boot to the log on screen
“Default“	means any breach of the obligations of the relevant Party (including but not limited to fundamental breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant Party or personnel including directors, officers, employees, sub-contractors, servants, agents and consultants in connection with or in relation to the subject-matter of the Contract and in respect of which such Party is liable to the other.
“**Defective Goods”**	has the meaning given under Clause 3.6 of Schedule 2 of these Call-off Terms and Conditions;

"Delay Payments"	means the amounts payable by the Supplier to the Customer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
"Delay"	means: a delay in the Achievement of a Milestone by its Milestone Date; or a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
“Desktop Device”	refers to a Lenovo Mini PC or other non-mobile desktop computer
“Desktop Device Bundle”	refers to a Desktop Device, monitor, keyboard, mouse, and appropriate cabling
“Device”	refers to the Authority’s tangible assets, including, but not limited to, desktop computers, laptops, 2-in-1 laptop and tablet devices
“DWP Place”	refers to the Authority’s IT Service Management tooling based on the ServiceNow product, previously known as TechNow
“Directive“	means EC Council Directive 2001/23/EC

"**Dispute Notice"**	means a written notice served by one Party to the other stating that the Party serving the notice believes there is a Dispute;
"**Dispute Resolution Procedure"**	means the process for resolving Disputes as set out in Clause 22 of Schedule 2 of these Call-off Terms and Conditions;
"**Dispute(s)"**	means any dispute, difference or question of interpretation or construction arising out of or in connection with this Contract, including any dispute, difference or question of interpretation relating to the Goods and Services, any matters of contractual construction and interpretation relating to the Contract, or any matter where this Contract directs the Parties to resolve an issue by reference to the Dispute Resolution Procedure;

"**DOTAS"**	means the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HM Revenue and Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to the National Insurance Contributions by the National Insurance Contribution (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.
"DPA"	means the Data Protection Act 2018
"**e Procurement Guidance"**	means the NHS eProcurement Strategy available via: http://www.gov.uk/government/collections/nhs-procurement together with any further Guidance issued by the Department of Health in connection with it;
"**Electronic Trading System(s)"**	means such electronic data interchange system and/or world wide web application and/or other application with such message standards and protocols as the Authority may specify from time to time;
"**Employment Liabilities"**	means all claims, demands, actions, proceedings, damages, compensation, tribunal awards, fines, costs (including but not limited to reasonable legal costs), expenses and all other liabilities whatsoever;

"**Environmental Regulations"**	shall have the meaning given to the term in Clause 1.2 of Schedule 3 of Appendix A Call-off Terms and Conditions;
"**Equality Legislation"**	means any and all legislation, applicable guidance and statutory codes of practice relating to equality, diversity, non - discrimination and human rights as may be in force in England and Wales from time to time including, but not limited to, the Equality Act 2010, the Part-time Workers (Prevention of Less Favourable Treatment) Regulations 2000 and the Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002 (SI 2002/2034) and the Human Rights Act 1998;
"Equipment"	means the Supplier's equipment, plant, materials and such other items supplied and used by the Supplier in the performance of its obligations under the Contract
"**Fair Deal for Staff Pensions"**	means guidance issued by HM Treasury entitled "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 (as amended, supplemented or replaced);
"**FOIA"**	shall have the meaning given to the term in Clause 1.2 of Schedule 3 of Appendix A Call-off Terms and Conditions;

"**Force Majeure Event"**	means any event beyond the reasonable control of the Party in question to include, without limitation: (d) war including civil war (whether declared or undeclared), riot, civil commotion or armed conflict materially affecting either Party's ability to perform its obligations under this Contract; (e) acts of terrorism; (f) flood, storm or other natural disasters; (g) fire; (h) unavailability of public utilities and/or access to transport networks to the extent no diligent supplier could reasonably have planned for such unavailability as part of its business continuity planning; (i) government requisition or impoundment to the extent such requisition or impoundment does not result from any failure by the Supplier to comply with any relevant regulations, laws or procedures (including such laws or regulations relating to the payment of any duties or taxes) and subject to the Supplier having used all reasonable legal means to resist such requisition or impoundment; (j) compliance with any local law or governmental order, rule, regulation or direction applicable outside of England and Wales that could not have been reasonably foreseen; (k) industrial action which affects the ability of the Supplier to supply the Goods and/or to provide the Services, but which is not confined to the workforce of the Supplier or the workforce of any Sub-Supplier of the Supplier; and (l) a failure in the Supplier's and/or Authority's supply chain to the extent that such failure is due to any event suffered by a member of such supply chain, which would also qualify as a Force Majeure Event in accordance with this definition had it been suffered by one of the Parties; but excluding, for the avoidance of doubt, the withdrawal of the United Kingdom from the European Union and any related circumstances, events, changes or requirements;

"**Forest Law Enforcement Governance and Trade (FLEGT)"**	means the facility that contributes to combating illegal logging and strengthening forest governance while encouraging sustainable economic development in countries that produce or process timber and export to the European Union.
"**Framework Agreement"**	means the Framework Agreement referred to in the Order Form;
"**Fraud"**	means any offence under any law in respect of fraud in relation to this Contract or defrauding or attempting to defraud or conspiring to defraud the government, parliament or any Contracting Authority;
"**GDPR"**	means the General Data Protection Regulation (Regulation(EU) 2016/679);
"General Anti-Abuse Rule"	means:- a) the legislation in Part 5 of the Finance Act 2013; and b) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions.

"**General Anti-Abuse Rule"**	means: (a) the legislation in Part 5 of the Finance Act 2013; and (b) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions;
"**General Change in Law"**	means a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply.
"Gold Stock"	refers to stock available for immediate deployment
"**Good Industry Practice"**	means standards, practices, methods and procedures conforming to the Law and the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar type of undertaking under the same or similar circumstances.
"**Good Industry Practice"**	means the exercise of that degree of skill, diligence, prudence, risk management, quality management and foresight which would reasonably and ordinarily be expected from a skilled and experienced supplier and/or service provider engaged in the manufacture and/or supply of goods and/or the provision of services similar to the Goods and Services under the same or similar circumstances as those applicable to this Contract; including in accordance with any codes of practice published by relevant trade associations;

"**Goods"**	means all goods, materials or items that the Supplier is required to supply to the Authority under this Contract; including tangible assets, such as Devices; Device Bundles; Monitors; Monitor Arms; standard catalogue peripherals, accessibility or non-standard catalogue items including peripherals
"**Guidance"**	means any applicable guidance, direction or determination and any policies, advice or industry alerts which apply to the Goods and Services, to the extent that the same are published and publicly available or the existence or contents of them have been notified to the Supplier by the Authority and/or have been published and/or notified to the Supplier by the Department of Health, Monitor, NHS England, the Medicines and Healthcare Products Regulatory Agency, the European Medicine Agency, the European Commission, the Care Quality Commission and/or any other regulator or competent body;
"**Halifax Abuse Principle"**	means the principle explained in the CJEU Case C-255/02 Halifax and others;
"ICT"	Information and Computer Technology.
"**Implementation Requirements"**	means the Authority's implementation and mobilisation requirements (if any), as may be set out in the Specification and Tender Response Document and/or otherwise as part of this Contract, which the Supplier must comply with as part of implementing the Services;

“Information Security Management System (“ISMS”)”	shall mean the set of policies, processes and systems designed, implemented and maintained by the Supplier to manage Information Security Risk as certified by ISO/IEC 27001.
“Information Security Manager”	shall mean the person appointed by the Supplier with the appropriate experience, authority and expertise to ensure that the Supplier complies with the Authority’s Security Requirements.
“Information Security Questionnaire”	shall mean the Authority’s set of questions used to audit and on an ongoing basis assure the Supplier’s compliance with the Authority’s Security Requirements.
“Information Security Risk”	shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.

"Information Security"	shall mean: the protection and preservation of: the confidentiality, integrity and availability of any Authority Assets, the Authority's Systems Environment (or any part thereof) and the Supplier's Systems Environment (or any part thereof); related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and compliance with all Law applicable to the processing, transmission, storage and disposal of Authority Assets.
"Information"	has the meaning given under section 84 of the FOIA.
"Initial Term"	Means the term the stipulated length of the contract on the Commencement Date.
"Intellectual Property Rights"	means patents, inventions, trade marks, service marks, logos, design rights (whether registerable or otherwise), applications for any of the foregoing, copyright, database rights, domain names, trade or business names, moral rights, goodwill and other similar rights or obligations whether registerable or not in any country (including but not limited to the United Kingdom) and the right to sue for passing off.

"**Intellectual Property Rights"**	means all patents, copyright, design rights, registered designs, trade marks, know-how, database rights, confidential formulae and any other intellectual property rights and the rights to apply for patents and trade marks and registered designs;
"**Interested Party"**	means any organisation which has a legitimate interest in providing services of the same or similar nature to the Services in immediate or proximate succession to the Supplier or any Sub-contractor and who had confirmed such interest in writing to the Authority;
"**International Organisation"**	shall have the same meaning as given in Data Protection Legislation.
"ISO/IEC 27001, ISO/IEC 27002 and ISO 22301	shall mean ISO/IEC 27001; ISO/IEC 27002/IEC; and ISO 22301 in each case as most recently published by the International Organization for Standardization or its successor entity (the "ISO") or the relevant successor or replacement information security standard which is formally recommended by the ISO.
"**Job Seekers"**	means people looking for work
"**Key Provisions"**	means the key provisions set out in Schedule 1 of these Call- off Terms and Conditions and/or as part of the Order Form;

"**KPI"**	means the key performance indicators as set out in the Specification and Tender Response Document and/or the Order Form, if any;
"Laptop Device"	refers to either a laptop or a 2-in-1 laptop and tablet device
"Laptop Device Bundle"	shall refer to a bundle consisting of a laptop device and selection of peripherals agreed during on-boarding

"**Law"**	means any applicable legal requirements including, without limitation,: (a) any applicable statute or proclamation, delegated or subordinate legislation, bye-law, order, regulation or instrument as applicable in England and Wales; (b) any applicable European Union obligation, directive, regulation, decision, law or right (including any such obligations, directives, regulations, decisions, laws or rights that are incorporated into the law of England and Wales or given effect in England and Wales by any applicable statute, proclamation, delegated or subordinate legislation, bye-law, order, regulation or instrument); (c) any enforceable community right within the meaning of section 2(1) European Communities Act 1972; (d) any applicable judgment of a relevant court of law which is a binding precedent in England and Wales; (e) requirements set by any regulatory body as applicable in England and Wales; (f) any relevant code of practice as applicable in England and Wales; and (g) any relevant collective agreement and/or international law provisions (to include, without limitation, as referred to in (a) to (f) above);
"Liquidation"	means the appointment of a Liquidator who collects in and distributes the company's assets and dissolves the company. The company can also be put into provisional Liquidation before a final winding up order is granted.
"**Long Stop Date"**	means the date, if any, specified in the Specification and Tender Response Document;

“**Loss“**	means direct loss, liabilities, claims, damages, costs, charges, outgoings and expenses (including legal expenses) of every description, provided in each case that such loss is reasonable, direct, proper and mitigated.
“**Material Breach”**	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform (of which the defaulting Party has been served a Breach Notice) as required under this Call-Off Contract.
“**Milestone"**	means an event or task described in the Implementation Plan which, if applicable, must be completed by the relevant Milestone Date;
"Milestone Date"	means the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved;
"Milestone Payment"	means a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone;
“**Implementation Plan”**	means the implementation plan, if any, referred to in the Key Provisions; meaning the Authority’s implementation and mobilisation requirements (if any), as may be set out in the Specification and Tender Response Document and/or otherwise as part of this Contract, which the Supplier must comply with as part of implementing the Services;
“Month“	means calendar month

“NCSC”	shall mean the National Cyber Security Centre or its successor entity (where applicable).
“**Older Worker“**	means a person 50 years of age and over.
“**Operational Change“**	means any change in the Supplier's operational procedures which in all respects, when implemented:- will not affect the Contract Price and will not result in any other costs to the Authority; may change the way in which the Services are delivered but will not adversely affect the output of the Services or increase the risks in performing or receiving the Services; will not adversely affect the interfaces or interoperability of the Services with any of the Authority’s Systems Environment; and will not require a change to this Contract.
Call-Off“ ”	means the agreement for the Goods and Services issued by the Authority in accordance with the Framework Agreement;
“**Party”**	means the Authority or the Supplier as appropriate and Parties means both the Authority and the Supplier;

“PCI DSS”	shall mean the Payment Card Industry Data Security Standard as most recently published by the PCI Security Standards Council, LLC or its successor entity (the “PCI”).
“Penetration Test”	shall mean a simulated attack on any Authority Assets, the Authority’s Systems Environment (or any part thereof) or the Supplier’s Systems Environment (or any part thereof).
“Service Manager”	which shall be identified by the Authority in the service Operations Manual, shall have monthly meetings to monitor and review the performance of this agreement
“TUPE"	means the Transfer of Undertakings (Protection of Employment) Regulations 2006 (2006/246) and/or any other regulations or other legislation enacted for the purpose of implementing or transposing the Acquired Rights Directive (77/187/EEC, as amended by Directive 98/50 EC and consolidated in 2001/23/EC) into English law;
“User”	shall refer to any person utilising the Devices supported by this contract

Addendum 1

Requirements

Category	Ref #	Requirement	Description	Scored or Mandatory
Device & Monitor Replace & Repair	1.1 a	Delivery and collection (Device)	The Supplier shall replace the faulty Device with a working equivalent, within the stated SLA standards detailed within Schedule 7B Call off Contract, at any UK location (including User homes). The Supplier shall make direct contact with the User to agree a date for the replacement and collection to take place and to obtain any additional information required. The replacement Device shall be delivered directly to a named User. The delivery of the replacement Device and the collection of the faulty Device shall be carried out as a single transaction. For the avoidance of doubt, a “working equivalent” refers to a Device from the appropriate Gold Stock that is asset tagged, newly built, powers on and boots to the DWP login screen, with the appropriate power cable. The Authority shall provide guidance as to what Devices are appropriate equivalents for each Device type upon contract award. In the case of a Desktop Device at an office, the Supplier shall de-install the faulty Device and install the replacement Device at the desk as requested. For the avoidance of doubt, this is not in scope for Laptops or home Users. Engineers performing installation activities must have BPSS security clearance. The Supplier shall securely package the collected Device for onward delivery. For the avoidance of doubt, the Supplier shall be responsible for the provision of packaging. The Supplier shall provide a courier service to return the Device to Supplier site. The courier service used for Devices must be secure, auditable, tracked and appropriately insured. The Supplier shall manage this service through the Incident Management process and using DWP Place. This includes updating the asset repository within 48 hours. The Supplier shall replace any Goods classed as Dead on Arrival (DOA) by the next business day following notification by the Authority. The Authority shall report any DOAs via the Incident Management process. For the avoidance of doubt Goods, including Devices, shall be provided under a separate Authority contract.	Scored Requirement
	1.1 b	Delivery and collection (monitor)	The Supplier shall replace the faulty monitor with a working equivalent, within the stated SLA standards detailed within Schedule 7B Call off Contract, at any UK location (including User	Scored Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			homes). The Supplier shall make direct contact with the User to agree a date for the replacement and collection to take place and to obtain any additional information required. The replacement monitor shall be delivered to a named User. The delivery of the replacement monitor and the collection of the faulty monitor shall be carried out as a single transaction. For the avoidance of doubt, a "working equivalent" refers to a monitor from the appropriate Gold Stock that is functioning and has the appropriate power cable. This shall be provided by a separate Authority contract. The Authority shall provide guidance as to what constitutes an appropriate equivalent for each monitor specification upon contract award. The Supplier shall securely package the collected monitor for onward delivery. For the avoidance of doubt, the Supplier shall be responsible for the provision of packaging. The Supplier shall provide a courier service to return the monitor to Supplier site. In the case of a monitor at office, the Supplier shall de-install the faulty monitor and install the replacement monitor at the desk as requested. For the avoidance of doubt, this is not in scope for home Users. Engineers performing installation activities must have BPSS security clearance. The Supplier shall manage this service through the Incident Management process (detailed within the attached document 9 – Incident Management Framework Policy) and using DWP Place. The Supplier shall replace any Goods classed as Dead on Arrival (DOA) by the next business day following notification by the Authority. The Authority shall report any DOAs via the Incident Management process.	
	1.1 c	Northern Ireland replacement service	Replacement services to DWP & Department for Communities (DfC), Northern Ireland shall be limited to a single weekly visit to address any outstanding incidents and replace broken Devices and monitors stored at the following locations: • Belfast CSAC • Belfast Benefit Center (Plaza) • Lanyon Place Belfast • Lisahally • Ballymena The activity performed for DWP's Northern Ireland offices and for DfC's offices shall both be invoiced separately. DfC replacement Devices must also be provided from the separate stock kept for DWP and DfC, with all Devices provided to DfC Users having a DfC asset tag. The Supplier shall complete any associated asset management activity within 48 hours.	Scored Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			For any shipments to and from Northern Ireland, the Supplier shall be responsible for the management of any associated customs activity.	
	1.2	Processing faults at Supplier site	The Supplier shall perform the following activities within the agreed service measures: **Assessment:** • Assessment, including diagnostic, of the defective Device • Basic-level assessment of the defective Monitor • Devices that successfully pass the assessment (diagnostic check) should be returned to Gold Stock. For the avoidance of doubt, the Device should be rebuilt to the latest Authority image before leaving the Supplier premises. • Monitors which pass the basic-level assessment and are fit for purpose should be returned to Gold Stock **Warranty:** • Where Devices and monitors do not pass the assessment and are within Warranty, the Supplier shall perform Warranty Management for both Device and monitors on behalf of the Authority • Replacement Devices shall be added into Gold Stock for redeployment, with the associated asset management activity carried out, detailing the faulty Device as corresponds with the replacement Device. • Replacement Devices must be built to the latest approved Authority build before leaving Supplier site **Repair:** • Out-of-warranty Devices must be repaired at a component level to industry standard. As a minimum this shall be using a skilled engineer. All repairs should be guaranteed for a minimum of 12 months. • Where possible, replacement components from previously decommissioned stock should be used • Repaired Devices to be added into Gold Stock for redeployment, with the associated asset management activity carried out. • Repaired Devices must be built to the latest approved Authority build before leaving Supplier site **Non-repair:** • Any Devices or monitors that the Supplier deems as Beyond Economical Repair, should be raised with the Authority. The Authority shall agree with the Supplier the appropriate route for these, either approving the repair or requesting the Device is moved to recycling/disposal as per the section 3 below entitled “End of Life Service” • Where applicable, the Supplier shall retain working components from the Devices identified for disposal to use as replacement components in future repairs	Scored Requirement
	1.3	Incident management	The Device and Monitor Replacement & Repair Services shall be enacted using the Authority’s Incident & Problem Management Processes (detailed within the attached; 6 - Incident Management	Mandatory Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			Framework Policy). The Supplier shall conform to DWP Incident Management Policies & Procedures, Processes & Standards.	
	1.4	Problem management	The Supplier shall perform trend analysis against incident and repair information. Any trends should be notified in accordance with the attached DWP Problem Management Framework policy, with recommendation for resolution of emerging issues. The Supplier shall be required to work in collaboration with the Authority and DWP third parties to investigate trends and any shift-left opportunities. The Supplier should notify the Authority of any industry knowledge with regards to known errors against common issues for the specific makes and models of Devices in use by the Authority.	Mandatory Requirement
	2.1	Request management service	The Supplier shall provide on-demand service capabilities including fulfilment of standard, non-standard and project requests including: • Adds (Joiners) • Moves • Change of Device type • Decommission (Leavers) • Disposal These shall be managed and controlled via the Authority's Request Fulfilment Policies & Procedures and using the Authority's DWP Place tooling (for further information please see 7 – Request Fulfilment Policy). The Supplier shall conform to Authority processes including updating of the asset repository and stockholding inventories.	Mandatory Requirement
Request Management	2.2 a	Adds (Desktop Devices)	The Supplier shall deliver from Gold Stock a Desktop Device Bundle that is asset tagged, newly built, powers on and boots to the DWP login screen. The Desktop Device Bundle shall be delivered directly to a named User at a specified UK location. The courier service used for Devices must be secure, auditable, tracked and appropriately insured. At an Authority office, the Supplier shall install or de-install the Desktop Device Bundle at the desk as requested. The Supplier shall ensure the Device is installed, useable and that the User can log on successfully. Engineers performing installation activities must have BPSS security clearance. The Supplier shall replace any Goods classed as Dead on Arrival (DOA) by the next business day following notification by the Authority. The Authority shall report any DOAs via the Service Request process. The Supplier shall manage this service using DWP Place. This includes updating the asset repository within 48 hours. For the avoidance of doubt, the Goods, including Devices and Peripherals shall be provisioned under a separate Authority contract	Scored Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
	2.2 b	Adds (Laptops)	The Supplier shall deliver from Gold Stock a Laptop Device Bundle that is built, asset tagged and functioning. The Laptop shall be delivered directly to a named User at a specified UK location. The courier service used for Devices must be secure, auditable, tracked and appropriately insured. The Supplier shall replace any Goods classed as Dead on Arrival (DOA) by the next business day following notification by the Authority. The Authority shall report any DOAs via the Service Request process. The Supplier shall manage this service using DWP Place. This includes updating the asset repository within 48 hours. For the avoidance of doubt, the Goods, including Devices and Peripherals shall be provided under a separate Authority contract.	Scored Requirement
	2.3	Moves	Moves at and between sites The Supplier shall provide an on-demand Move service capability. These shall be managed and controlled via the Authority's request management processes using the Authority's DWP Place tooling. The Supplier shall provide this service for the following items: • Desktop Device Bundle • Monitor (with or without a monitor arm) • Moves at a site: o The Supplier shall de-install the requested Bundle and re-install it at a different desk elsewhere at the Authority site • Moves between sites: o The Supplier shall de-install the requested Bundle from the desk and package it up for onward delivery. The Supplier shall be responsible for the provision of appropriate packaging. o The Supplier shall deliver the requested Bundle to the requested site. The courier service used must be secure, auditable, tracked and appropriately insured. For a monitor, a standard courier is acceptable. o The Supplier shall install the requested Bundle at the desk. Engineers performing installation activities must have BPSS security clearance. The Supplier shall manage this service using DWP Place tooling. This includes updating the asset repository within 48 hours.	Scored Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
	2.4	Changes	The Supplier shall provide an on-demand Change service capability. These shall be managed and controlled via the Authority's request management processes using the Authority's DWP Place tooling. This service shall be called upon to change a User's Device type. As a single transaction, the Supplier shall perform a decommission as per the section entitled "Leaver" and an add as per the sections entitled "Adds (Desktops)" or "Adds (Laptops)" (dependent on Authority request). Engineers performing installation activities must have BPSS security clearance. The Supplier shall manage this service using DWP Place tooling. This includes updating the asset repository within 48 hours.	Scored Requirement
	2.5	Leaver	The Supplier shall provide an on-demand Leaver service. This shall entail collection of Devices or Device Bundles from a UK address. At an Authority office, the Supplier shall de-install the Desktop, Laptop or Monitor at the desk as requested. Engineers performing installation activities must have BPSS security clearance. For all Devices, the Supplier shall securely package the collected item for onward delivery. The Supplier shall be responsible for the provision of appropriate packaging. The Supplier shall provide a courier service to return the item to Supplier site. The courier service used for Devices must be secure, auditable, tracked and appropriately insured. For a monitor, a standard courier is acceptable Once at Supplier site, the Supplier shall clean and rebuild (where applicable) the item and return it to Gold Stock. The Supplier shall manage this service using DWP Place tooling. This includes updating the asset repository within 48 hours.	Scored Requirement
	2.6 a	Installation (Optional)	The Supplier shall provide an on-demand, optional Engineering/Installation service capability at all UK addresses including fulfilment of standard, non-standard and project requests. These shall be managed and controlled via the Authority's request management processes using the Authority's DWP Place tooling. The Supplier shall provide suitably skilled resources in order to install Devices, monitors, and Device Bundles. Engineers performing installation activities must have BPSS security clearance. The Supplier shall co-ordinate and manage these requests within agreed SLAs. **Achievement Criteria:** The Supplier shall ensure the Device is securely and safely installed by carrying out the activities included, without limitation, below:	Scored Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			• Fixing securely the monitor onto the monitor arm or stand • Ensuring that all peripherals are correctly connected to the Device chassis or the appropriate docking station • Ensuring that the Device is correctly connected to the power and network • Ensuring that all cables are safe, tidy, and suitably secured in accordance with good industry practice and standards • All packaging is removed to ensure the area is returned to its pre-installation state • Ensuring that each Device deployed successfully starts and presents the Authority log-in screen • Where a Device is discovered to be DOA during installation, the Supplier shall remove the DOA Device and return to install a working Device by the next business day. • For Devices, update the asset repository within 48 hours.	
	2.6 b	De-Installation (Optional)	The Supplier shall provide an on-demand, optional Engineering/de-Installation service capability at all UK addresses including fulfilment of standard, non-standard and project requests. These shall be managed and controlled via the Authority's request management processes using the Authority's DWP Place tooling. The Supplier shall provide suitably skilled resources in order to de-install Devices, monitors, and Device Bundles. Engineers performing installation activities must have BPSS security clearance. The Supplier shall co-ordinate and manage these requests within agreed SLAs. **Achievement Criteria:** The Supplier shall ensure the Device is securely and safely de-installed by carrying out activities included, without limitation, below: • Providing appropriate packaging for onward shipment of the Device to a UK location • Unplug Devices and peripherals and securely package for removal • For Devices, update the asset repository to a state of "in transit" within 48 hours. The Device shall then be handled as per the requirements in either the section entitled "Moves" or the section entitled "Leaver", as per the Authority's request.	Scored Requirement
	2.7	Non-standard service requests	A Non-Standard Service Request shall be used for desktop-related services that are usually Standard Service Catalogue items that are greater than agreed standard volumes, take place in out-of-core hours, or require specific completion times. Upon receipt of a request from the Authority, the Supplier shall confirm to the requestor within 2 working days whether the request is a Non-Standard Service Request or a Project Request and when a quote should be expected For Non-Standard Service Requests the Supplier shall provide a quote within 3 working days. This response shall include, without	Scored Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			limitation, pricing for the request and the expected date of the service provision. The Authority may submit an expedited Non-Standard Service Request for which the Supplier is asked to quote and complete in as short a timescale as is reasonable. These shall be an exception. The Supplier shall provide a monthly report of completed Non-Standard Service Requests including the final costs associated and whether they were completed within quoted timescales and prices. The format of this report shall be agreed by the Authority and the Supplier during on-boarding. Developments are currently underway to enable the management of Non-Standard Service Requests through DWP Place. Until these changes are made, the Supplier shall manage Non-Standard Service Requests via e-mail. Once these changes are made, the Supplier shall manage this service using DWP Place tooling. This includes updating the asset repository where appropriate within 48 hours.	
	2.8	Project requests	A Project Request is a piece of work being run as a project that requires additional management across various strands of activity. These may constitute a new service line and become included in the contract as a contract variation. The Supplier shall provide a full quote within 15 working days of receiving the request from the Authority, including, without limitation, pricing and timescales for the request. The Authority may request an indicative quote within 5 working days of submitting the request: this shall be an exception. The Supplier shall provide a monthly report of completed Project Requests including the final costs associated and whether they were completed within quoted timescales and prices.	Scored Requirement
End of life service	3.1	End of life service	The Supplier shall provide an on-request end of life service to consider the most appropriate approach for dealing with Goods that are no longer required or functioning. This shall include options for disposal, recycling, and resale. This shall be managed via the Authority's request management processes and DWP Place tooling. For the avoidance of doubt, any Device that is decommissioned but still required and functioning shall be returned to stock ensuring DWP processes are followed including updating of asset repository in DWP Place within 48 hours. The Authority shall advise the Supplier of Devices that are no longer required.	Mandatory Requirement
	3.2	Recycling and resale	Prior to any disposal decision, the Supplier shall make an assessment of the Devices to consider whether the Device or any working components can be utilised in repairs or whether there is potential for recycling or resale. The Supplier shall provide the Authority with recommendations and indicative resale value. Following completion of a resale request, the Supplier shall provide a report detailing items resold	Scored Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			and actual resale value. The approach to managing the resale value shall be established and defined as part of on-boarding. If the Authority approves that a Device is to be recycled or resold, the Supplier shall securely wipe the Device. Device sanitisation will be managed by the Supplier, utilising an automated task sequence in the Authority's SCCM toolset. When managing any recycling or resale of Devices, the Supplier shall: · Follow NCSC guidance found at https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media · Follow CPNI Standard for Secure Destruction of Sensitive Items found at: https://www.cpni.gov.uk/system/files/documents/c5/e1/2017_01_20_CPNI_Secure_Destruction_Standard.pdf The Authority shall perform periodic audits to confirm Supplier adherence to NCSC and CPNI standards and guidance. The Supplier shall provide asset and model details to the Authority within 48 hours of removal of stock from DWP usage.	
	3.3	Disposal	Goods shall be disposed of in accordance with all applicable Standards, Policies & Procedures including any relevant Standards in respect of sustainability, data security, health and safety, the Waste Electrical and Electronic Equipment (WEEE) Regulations and CD Electronic Media reuse and disposal standards. The Supplier shall ensure that the Supplier or partner who disposes of the Authority's Devices are Commodity Assurance Services (CAS) certified by National Cyber Security Centre (NCSC). In relation to data security, the Supplier shall: · Follow NCSC guidance found at https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media · Follow CPNI Standard for Secure Destruction of Sensitive Items found at: https://www.cpni.gov.uk/system/files/documents/c5/e1/2017_01_20_CPNI_Secure_Destruction_Standard.pdf The Authority shall perform periodic audits to confirm Supplier adherence to NCSC and CPNI standards and guidance. The Supplier shall seek Authority approval prior to their secure destruction service and provide details of the reason(s) why it is not economically advantageous to repair the Device. • If the Authority approves that a Device is irreparable and not to be held as decommissioned stock, the Supplier shall securely wipe the Device. • The Supplier shall provide the asset and model details to the Authority so they can update the asset repository within 48 hours of removal of stock from DWP usage. • As requested by the Authority, the Supplier shall review Goods scheduled for destruction to understand whether	Scored Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			there is any residual value and propose options to recover this residual value. • Where a Device is scheduled for destruction, the Supplier shall take an appropriate stock of replacement components from the Device for use in repairs of other Devices. • Disposals shall be managed in accordance with WEEE regulations and CD Electronic Media reuse and disposal standards. The Supplier must provide the relevant disposal certification. • The Supplier shall ensure that disposal decisions are maintained utilising the Authority's tooling (DWP Place). • The Supplier shall, within 48 hours of disposal, provide to the Authority the Certificate of Destruction (including reference), asset details and model of the disposed Devices.	
Close-to-box services	4.1 a	Build – Device Specific Image Creation, Configuration	The Authority shall provide, at contract award: • A copy of an existing Windows 10 image that has been tested to ensure that it works with Devices currently deployed on the Authority's infrastructure. • A copy of an existing Paradox image that has been tested to ensure that it works with Devices currently deployed on the Authority's infrastructure. The Authority shall provide the image to the Supplier on approved build sticks (USB Device) as part of the early mobilisation activities. The Supplier shall not modify the Authority's Windows 10 image or Paradox image. The Supplier shall, within two (2) weeks of Contract Award be able to deliver on the DWP Devices, the Authority's Windows 10 image and Paradox image. In the event that the Supplier encounters any issues relating to either build, they shall raise these issues with the Authority and work in conjunction with the Authority to resolve those issues. The Supplier's image build facility shall be located in the UK. The Authority, prior to delivery of any Goods under this Contract shall assess the build facility. The Authority shall require access to the Supplier's site in order to complete this assessment. The Supplier is to provide security service description(s) they are offering with regards to the degree of separation between work for DWP and their other customers in an air-gapped environment as part of their tender response. The Supplier resources who handle the image build processes shall have SC clearance. For information, this requirement is likely to be affected by the planned joint work during the life of this contract as the Authority adopts a CloudFirst approach to Device provision, as covered off in the section entitled "CloudFirst Devices".	Scored Requirement
	4.1 b	Build – Device Authority Testing	The Authority shall test the Device and the updated image provided by the Supplier using pre-defined test scripts to ensure it meets the Authority's requirements. The Authority shall share test	Scored Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			scripts at the commencement of the Contract. It is anticipated that the Authority's testing shall take three (3) days.	
	4.1 c	Build –Device IT Health Check	The Supplier (if required) shall provide support to an IT Health Check (ITHC) of the Authority's Windows 10 image and the Authority's Paradox image. The ITHC shall be undertaken by an independent third party and the appointment shall be at the Authority's discretion. It is anticipated that Authority testing and ITHC may take up to two (2) weeks. The Supplier may be required to complete remedial activities, at no additional charge, as a result of the ITHC.	Mandatory Requirement
	4.1 d	Build/Re-build	The Supplier shall ensure any Devices that are deployed are up to date with the latest build provided by the Authority, including DWP-approved system patches via SCCM. For Paradox, the Supplier shall be provided with USB sticks by the Authority, which will update to the latest build automatically when the Supplier refreshes the system updates. For the avoidance of doubt, the Supplier shall undertake the build. The Supplier shall confirm the Devices successfully boot to logon screen. Any Devices which fail checks should be reported back to the Authority advising of asset details to confirm warranty replacement or rebuild.	Scored Requirement
	4.1 e	Build – Image Updates	The Supplier shall apply the approved image as detailed in the requirement detailed above or the version agreed with the Authority (as updated from time to time) to all Devices prior to delivery to the relevant site and in accordance with the Implementation Plan and Specific Site Order. In the event that the builds or Authority's infrastructure changes, the Authority shall inform the Supplier via the service management change process. The Supplier shall within 5 working days have completed testing and, working with the Authority, confirmed acceptance and implemented the new build. Image updates shall be subject to strict change and version control. The Authority shall provide image updates to enable the Supplier to deploy onto the Devices before delivery.	Scored Requirement
	4.1f	CloudFirst Devices	Through the term of this Contract, the Authority shall be introducing CloudFirst Devices. The Supplier shall support the Authority in reviewing and revising its service delivery and support model to accommodate the emerging CloudFirst estate. The Supplier shall evidence where they have implemented or are implementing CloudFirst for another customer, and how they shall support the Authority in doing so.	Scored Requirement
	4.2	Asset tag service	The Supplier shall be responsible for accurately and securely asset tagging Devices. The Supplier shall provide record of each Device's asset number versus its serial number and ensure that these records accurately match the physical serial number and asset number of each Device. Asset tagging must be undertaken on each Device before leaving the Supplier's premises in accordance with the Policy and Standards (and its updates from time to time). For the avoidance of doubt, the Supplier shall provide the physical asset tags which must comply with the Authority's Asset Tagging Policy.	Scored Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			There are different asset tags for DWP and DfC and the Authority shall notify the Supplier which asset tags to use for each Device serial number range.	
Capability, Capacity & Social Values	5.1	Capability and Capacity	**Capability and Capacity** The Supplier shall have the Capability and Capacity to meet the Services as detailed in the specification, in order to support bulk deployment, decommission, recycling, disposal and refresh projects. The Supplier shall have the Capability to meet specific Project and Transformation requests and the Capability and Capacity to flex up and down in order to meet these requirements, including but not limited to: - Goods in processes - Goods out processes including bundling Goods for ease of delivery to end Users - Warehousing Capability and Capacity - Build Capability and Capacity - Flexibility of Logistics to meet emerging demand - Re-use including cleaning, re-build and storage - Re-cycling and WEEE disposal	Scored Requirement
	5.2	Logistics (Optional)	The Supplier shall provide an on-demand logistics service covering the movement of IT kit from one UK location to another. This shall include, but not be limited to: • Movement of full Device Bundles in single or bulk quantities • Movement of specified Devices or peripherals in single or bulk quantities • Option for timed delivery including specific one-hour slots, pre-9:30am delivery and pre-noon delivery. • Options for both secure and standard couriers Where this logistics service is requested at a Northern Ireland location, the Supplier shall manage all associated customs activity.	Scored Requirement
	5.3	Social Values	The Supplier shall provide detail of how they ensure social values are prioritised within their organisation. The Supplier shall be evaluated on the following Social Values: **COVID-19 recovery:** • Help local communities to manage and recover from the impact of COVID-19 **Tackling economic inequality:** • Create new businesses, new jobs and new skills • Increase supply chain resilience and capacity **Fighting climate change:** • Effective stewardship of the environment. • Please note, this will be evaluated as part of the End of Life service section rather than as a separate social value **Equal opportunity:** • Reduce the disability employment gap • Tackle workforce inequality	Scored Requirement

<table>
<tr><th>Category</th><th>Ref #</th><th>Requirement</th><th>Description</th><th>Scored or Mandatory</th></tr>
<tr><td></td><td></td><td></td><td>Wellbeing:
Improve health and wellbeing
Improve community cohesion</td><td></td></tr>
<tr><td>Underpinning requirements</td><td>6.1</td><td>Asset management – asset repository</td><td>The Supplier shall comply with mandatory The Authority's Asset Management Policies, to ensure Devices can be tracked at all stages of the asset management lifecycle, and that the Authority can account for all Devices both physically and virtually.

The Authority's Asset Management Policies must be followed and acted upon by the Supplier whenever they handle a Device. The Supplier shall access the DWP Asset Repository in DWP Place to make the change to the relevant asset record within 48 hours. Throughout the service period, the Supplier shall perform regular checks of all moves in and out of the Physical and Virtual asset repositories and correct any errors made within 48 hours.

Devices are tracked in the DWP Place Asset Repository using virtual 'Stockrooms' allocated to the Supplier (or Authority team) who shall be responsible for ensuring Devices in the virtual Stockroom mirror Devices in the Supplier's physical Stockroom by serial number. The virtual 'Stockrooms' are used when a Device is not assigned to a User or DWP location.
It is imperative that the Supplier ensures that the serial numbers of the Devices held physically by the Supplier accurately match those held in the DWP Asset Repository.
The state and sub-state of the Device must also be captured in the asset record such as:

<table><tr><th>State</th><th>Sub-State</th></tr><tr><td>In Stock</td><td>Available</td></tr><tr><td>In Transit</td><td>Reserved</td></tr><tr><td>In Use</td><td>Defective</td></tr><tr><td>In Maintenance</td><td>Pending_Repair</td></tr><tr><td>Retired</td><td>Pending_install</td></tr><tr><td>Missing</td><td>Pending_disposal</td></tr><tr><td></td><td>Pending_transfer</td></tr><tr><td></td><td>Disposed</td></tr><tr><td></td><td>Lost</td></tr><tr><td></td><td>Stolen</td></tr></table><u>Bulk Moves of Devices</u>
Where the Supplier is moving a large quantity of Devices to another Stockroom, they can provide the asset details, Manufacturer, Model and Serial Number to the Authority Asset Management team who shall move the Devices on behalf of the Supplier.

Documented Asset Management processes of every stage and requirement are available to the Supplier and full training shall be provided by the Authority to Supplier staff.

The Supplier shall provide a monthly report to the Authority to demonstrate the thoroughness and accuracy of the Asset Management of Devices moving in and out of their stockroom. This report shall be based on a monthly Supplier audit to reconcile the content held in the Supplier's Physical stockroom with that recorded in the DWP Asset repository; the audit shall be</td><td>Mandatory Requirement</td></tr>
</table>

Category	Ref #	Requirement	Description	Scored or Mandatory
			managed, and reporting provided, to always include Device serial number to enable Departmental validation across the Physical and Virtual repositories. The Authority shall validate accuracy of reporting by sample-checking but shall also perform an audit of the Supplier's physical repository where necessary. For the avoidance of doubt, where the Supplier is unable to access DWP Place Asset Repository they are still responsible for ensuring asset records are updated by providing the Authority with full details of assets and relevant amendments.	
	6.2 a	Stockholding Services	The Authority is responsible for provision of the physical stock, utilising Authority supply contracts, to meet the ongoing Device and peripheral demand. The Authority shall provide a forward view of anticipated demand to the Supplier in a format and frequency to be agreed as part of on-boarding. For the avoidance of doubt, the Supplier shall not charge the Authority for holding any stock that has entered either into the warranty or repair loop. The Supplier shall not charge the Authority for holding any stock that facilitates the contract's service provision, including projects.	Mandatory Requirement
	6.2 b	Stockholding services – Stock Management and Reporting	The Supplier shall provide timely stock information on all Authority Goods held at the Supplier's site to ensure that the Authority can meet their responsibility, and this shall include the Supplier's demand and fulfilment requirements for Incident and Request Management Services. This shall be provided at the following frequency: • Weekly view to include the total volume of stock held at the Supplier site and status, e.g., in Gold Stock ready for call off, under repair • 3 month rolling view based on historical and volume analysis As part of the contract's governance, the Supplier shall attend a Monthly meeting with internal and, where applicable, external Suppliers in order to assist the Authority in managing Demand and to ensure effective Stock Management. As part of on-boarding and regular Demand Management reviews, the Supplier and the Authority shall jointly agree thresholds of stock levels at which the Supplier shall alert the Authority to provide further stock.	Mandatory Requirement
	6.3	Warehouse management capability	The Supplier shall store the Authority's Goods in a secure and identifiable manner and be able to track Goods at the Supplier site (including any Third Parties) involved in delivering this service. The Supplier shall ensure that DWP, Health Transformation Project and DfC Goods are stored separately and distinctly. There may be amendments to this list from time to time. The Supplier shall store, within Gold Stock, Device & Monitor Replacement Service Stock and Request Management Stock separately.	Mandatory Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			The Authority and Supplier shall agree appropriate stock levels for fulfilling the Device & Monitor Replacement Service and Request Management Service as part of on-boarding and regular discussions at Service Reviews. The Supplier shall also, on request, store Project Stock separately from Gold Stock. The Authority shall have the right to audit all of its Goods held at the Supplier's warehouse. Notice of 10 working days will be given ahead of any audit.	
	6.4	Reporting	The Supplier shall provide frequent reporting as detailed in the Appendix 10 of the attached Schedule 7B Call off Contract.	Mandatory Requirement
	6.5	Utilising DWP tools (inc. ITSM, DWP Place)	The Supplier shall use DWP Place tooling in delivery of services associated with this contract. For the avoidance of doubt, Supplier resources accessing DWP place must have Security Clearance to the minimum of BPSS. Supplier must confirm their compliance with the Code of Connectivity, as detailed here and provided along with this ITT. Please note, where reference is made to "TechNow", DWP Place is meant: The Supplier shall be subject to an IT Health Check. The Authority's tooling (DWP Place, DWP's ServiceNow instance) is provided by DWP via access through a dedicated URL via the Internet: this is subject to the Supplier passing the Authority's ITHC. For the avoidance of doubt, access cannot be from outside of the United Kingdom. On-boarding to DWP Place shall form part of Mobilisation. The Code of Connectivity (CoCo) summarises the requirements for a third-party Supplier to connect from their corporate infrastructure directly to the DWP Place Service Management tool. Code of Connectivity Summary The Supplier shall agree to their corporate build – image load – Device being assured for connectivity to the Department's tooling including a penetration test to be performed by an approved Security Tester under an agreed testing standard as agreed by the ESRM Security Risk Lead against their corporate Device build – image load. • The Device should be configured in a secure manner using the CESG End User Devices Security Guidance located at the following URL. Versions are also available for other operating systems from the same website. https://www.ncsc.gov.uk/guidance/end-user-device-security • The browser on the Device which is used to access the Department's tooling must be configured to use TLS 1.2 as a minimum.	Mandatory Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			• USB storage Device access should be appropriately managed. Where possible this should be locked down so as to become unusable but, where this is not feasible, the Supplier shall confirm to the Department that all Users of the Department's Services have agreed to procedures acknowledging the prohibition of using USB storage Devices to transfer data to or from these Services. If local working practices specifically require this type of working, then the Supplier shall demonstrate the process being used to the Department and seek a waiver which may be approved on a case-by-case basis. • The Supplier, in agreement with the Authority, shall be responsible for arranging the penetration testing prior to the Department allowing connectivity. Once this has been done the Department shall need to see the output and sign off the connectivity. • The Supplier shall be responsible for the cost of this assurance exercise and for carrying out any remedial activities as identified by and in agreement with the ESRM Security Risk Lead. • The scope of the test shall be against the CESG End User Devices Security Guidance for the Supplier's corporate build(s) – image load(s) • The purpose of the audit shall be to ensure that the Device is secured correctly (regular patching, has no known vulnerabilities, has up-to-date anti-virus, malware, etc.). • The Department reserves the right to carry out future checks for compliance. Typically, the penetration test shall need to be carried out on an annual basis or if there are any major build – image load – changes to the end Device. It is the Suppliers' responsibility to inform the Department if there are any major changes to their corporate build – image load, e.g., new OS or security component and for arranging the required penetration test. • Suppliers' staff are not allowed to use a personal Device at any time to access DWP Place.	
	6.6	Invoicing	The Supplier must provide accurate invoices and supporting Management Information on a monthly basis. The Authority shall create a Purchase Order (PO) per service line which the Supplier must invoice accurately against. In the case of the Supplier invoicing against the incorrect Purchase Order, the Authority will reject the invoice. The Supplier shall ensure that any invoice or credit note includes, without limitation, the following information: 1. The Purchase Order reference 2. The date of the invoice 3. A unique, numerical invoice number 4. The period to which the charges relate 5. Details of the correct contract reference 6. A contact name and telephone number of a responsible person in the Supplier's Finance department in the event of any administrative queries	Mandatory Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			7. The banking details for payment to the Supplier via electronic transfer of funds (i.e., name and address of bank, sort code, account name and number) 8. Clear indication of whether it is a credit note or invoice a. In the case of a credit note, detail of the invoice number the credit note is being raised against 9. The amounts charged, broken down at a summary level and matching the amounts detailed in the Management Information outlined below Where any invoice or credit note does not conform to the Authority's requirements detailed above and therefore does not constitute a valid invoice or credit note, the Authority will reject this invoice or credit note. Any invoice or credit note shall be accompanied with Management Information (MI), the format and content of which shall be agreed during the on-boarding process. This MI shall include, without limitation, the following information: 1. The dates upon which the services being charged were performed 2. Detail of the services being charged including volumes and unit costs 3. The methodology applied to calculate the charges 4. The invoice and Purchase Order reference that the MI corresponds to The Supplier shall submit, as soon as possible and in any case within ten (10) Working Days after the end of each calendar month, all invoices and accompanying Management Information in such format as the Authority may specify from time to time, for the Charges incurred during that calendar month. Invoices and credit notes shall be submitted to: • APinvoices-DWP-U@gov.sscl.com • workplacecomputing.invoices@dwp.gov.uk With all supporting documentation and management information also submitted to: • workplacecomputing.invoices@dwp.gov.uk At the point that the Authority notes a discrepancy in the billing, the Supplier shall respond within 3 working days with agreement or with further clarification. Discrepancies must be settled by the Supplier in the form of a credit note within 3 working days of such agreement. If this credit note is not raised within 10 working days of such agreement, the Authority may reject the invoice and ask the Supplier to re-invoice for the correct amount. The Authority shall have 6 months in which to raise any billing discrepancies. Any discrepancies raised after this point shall not be liable for remedy by the Supplier. For the avoidance of doubt, this 6-month deadline shall only apply where the Supplier has responded to invoicing queries within the agreed timescales outlined above.	

Category	Ref #	Requirement	Description	Scored or Mandatory
			The Supplier must provide any invoices to the Authority within 6 months of the completion of delivery of the relevant Services to which the invoice relates. Invoices delivered after expiry of this period shall be invalid and the Authority shall have no liability in respect of such invoices.	
	6.7 a	Mobilisation Plan	The Supplier shall provide a Mobilisation Plan and work with stakeholders to on-board and transition the required Services. The Supplier shall also produce an organisational structure for the relevant team with roles and responsibilities, assisting DWP in driving the service on-boarding activities. The Authority shall work with the Supplier to agree a mobilisation schedule based on work strands, people, tooling, processes, operational readiness and achievement of milestones. It is expected that this shall be within 3 months. The Mobilisation Plan shall include but not be limited to, the following as applies to each of the 3 service lines (Device & Monitor Repair & Replace, Request Management, Projects): • Key activities, timescales, risks, issues and dependencies • Resources and capabilities – including SMEs • Processes and procedures • Tooling • Proposed Service Commencement date to be agreed with the Authority The Supplier shall work with the Authority to develop an Operations Manual that describes all processes and procedures for the delivery of the service. The Authority and the Supplier shall jointly develop the governance approach for transition and on-boarding, working with the current incumbent Supplier where appropriate.	Scored Requirement
	6.7 b	Mobilisation Plan – Set up Costs	The Supplier shall confirm the one-off cost for mobilisation of this service for completeness. For the avoidance of doubt, this cost shall not be formally evaluated within the tender process, but the Authority shall review and a comparison across bidders shall be completed to ensure parity	Mandatory Requirement
	6.7 c	Mobilisation Plan – Transitional Arrangements	The Supplier shall collaborate with the Authority's previous Supplier to develop a service transition plan that runs sequentially with the previous Supplier's exit plan.	Mandatory Requirement
	6.7 d	Mobilisation Plan - Security	The Supplier shall confirm acceptance of Security Policies and Standards as linked to below: https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards The Authority shall work with the preferred Supplier to complete the mandatory security questionnaire and Cyber Essentials certificate The Supplier shall allow the Authority full access to its premises, including third-party supplier premises where appropriate, to complete an audit to meet the Authority's security requirements.	Mandatory Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
	6.7 e	Service Commencement Date	For the avoidance of doubt, the Authority shall not carry over incidents or requests raised prior to Service commencement; these shall be completed by the current incumbent Supplier. The Supplier shall only be responsible for incidents and requests raised on or after the Service Commencement Date.	Mandatory Requirement
	6.7f	Exit Plan	On the first-year anniversary of the contract, the Supplier shall provide the Authority with an updated outline exit plan.	Mandatory Requirement
	6.8	Account Management	• The Supplier must provide details of persons responsible for the management of the Contract. Key Supplier team members and team structure shall be confirmed as part of on-boarding. • Changes of persons responsible for the management of the Contract during its lifetime must be communicated 10 Working Days in advance of the change taking effect • Key Supplier team members cannot be moved to other Supplier accounts without agreement from the Authority. • Where there are significant issues with key Supplier team members the Authority reserves the right to ask for these to be replaced	Mandatory Requirement
	6.9	Co-ordination, Management and Control	The Supplier shall be responsible and accountable for managing the full end to end Supplier delivery teams, including partners/SMEs to minimise impacts including financial impacts on the Authority. The Supplier shall take full accountability for their supply chain performance by: • Understanding the full supply chain processes and delivery touchpoints • Regularly reviewing supply chain performance and implementation of improvement activity • Pro-actively engaging to anticipate and rectify service issues The Supplier shall collaborate with the Authority Third-Party Suppliers to ensure seamless integration of services including but not limited to checking in stock provisioned through third parties.	Mandatory Requirement
	6.10	Governance & Performance Management	The Supplier shall confirm their ability to work with the Authority in managing the services jointly, providing regular performance reporting. • The Supplier shall attend the range of Governance meetings detailed in the Governance meeting pack contained within Appendix 17 of the attached Schedule 7B Call off Contract. Key stakeholders for these meetings shall be defined in the Operations Manual. • The Supplier must provide management information to meet the reporting requirements detailed in the Terms & Conditions, meeting the specified scope and frequency. • As input into the weekly Operational Reviews, they shall provide a report showing performance of all SLAs and KPIs against targets. Additionally, they shall provide a forecast of the anticipated performance for the entire month. • As input into the monthly Service Review, the Supplier shall provide a Service Review pack including service level and management information showing the status of SLAs versus targets (unmitigated and mitigated), service	Mandatory Requirement

Category	Ref #	Requirement	Description	Scored or Mandatory
			highlights and lowlights, and narrative for additional activities. The delivery of the Service Review pack shall be expected on the fifth Working Day of the month relating to service in the previous month. • The Supplier shall conform to all SLAs and KPIs detailed within Appendix 10 of the attached - Schedule 7B Call off Contract. ○ The Supplier must highlight any instances of any failed SLA requirement in the monthly reporting information regardless of how many instances	
	6.11a	Service Management - Personnel	The Supplier shall be able to demonstrate the Service Leadership aligned to the account are formally qualified to high standard in Service Management methodologies (e.g., ITIL4 / AGILE). The supporting Service team shall have at least foundation qualifications in the same area. The Supplier shall align an industry-certified Project Manager to the account.	Mandatory Requirement
	6.11b	Service Management – Continuous Service Improvement	The Supplier shall agree with the Authority a minimum of x2 Continuous Service Improvement initiatives to be delivered per quarter. This shall be tracked and reviewed at the Monthly Service Review against proposed outcomes and benefits. The Supplier shall perform quality checks against a random sample of Incidents and Service Requests (minimum 5%), to ensure Good Practice and DWP Policies and Procedures are being adhered to. This should be evidenced to the Authority at the Monthly Service Review. With remediation actions recorded and completed where required.	Mandatory Requirement
	6.11c	Service Management – Quality Assurance	The Supplier shall assure the quality of service provided. Quality checks against a random sample of Incidents, Service Requests, Assets handled, and Repairs shall be performed monthly to ensure Good Practice and adherence to DWP Policies and Procedures. The number of Quality observations should be no less than 5% of the volume handled within the month. This should be evidenced to the Authority at the Monthly Service Review. With remediation actions recorded and completed where required.	Mandatory Requirement
	6.12	Policies & Procedures	The Supplier shall confirm adherence to all Policies, Procedures and Guidance as detailed throughout this document and below: • Asset Tagging Policy • Asset Management Policies & Procedures • Security Policies & Procedures, including GDPR • Change Management Policies and Procedures • Security Policies and Standards • Request Fulfilment Policies & Procedures • Problem Management Framework • Incident Management Framework • Code of Connectivity	Mandatory Requirement

Addendum 2 – CDW Commercial Response

The pricing model selected for the Device & Monitor Repair & Replace service will be a Fixed Price arrangement based upon the tender submission. The Authority reserves to right to vary that model in the future and will enter into good faith negotiations with the supplier to see if varying the model provides best value for money and improved delivery of services.

In respect of the prices provided for Request Management Non Standard, Request Management Projects and Bulk Transformation it is recognized that the pricing provided at the tender process, embedded, were based upon scenarios and not actual quantities for evaluation purposes. These prices will be used for benchmarking purposes for any future activity that the Authority may contract with the Supplier.

[REDACTED]

Addendum 3 – CDW Technical Response

[REDACTED]

Addendum 4 – CDW Response Clarifications

[REDACTED]

Addendum 5 – Change Control Forms

1. ANNEX 1 CHANGE

REQUEST FORM

CR No.:	Title:	Type of Change:

Project:	Required by Date:

Action:	Name:	Date:

Raised By:	
Area(s) Impacted (Optional Field):	
Assigned for Impact Assessment By:	
Assigned for Impact Assessment To:	
Supplier Ref. No.:	
Full Description of Requested Contract Change:	
Details of Any Proposed Alternative Scenarios:	
Reasons for and Benefits and Disadvantages of Requested Contract Change:	

Signature of Requesting Change Owner:	
Date of Request:	

ANNEX 2

Impact Assessment Form

CR No.:	**Title:**	**Date Raised:**
Project:		**Required by Date:**

Detailed description of Contract Change for which Impact Assessment is being prepared and details of any related Contract Changes:	
Proposed adjustment to the Charges resulting from the Contract Change:	
Details of proposed on-off additional charges and means for determining these (e.g. Fixed Price or Cost-Plus basis)	
Details of any Proposed Contract amendments:	
Details of any Service Levels affected:	
Details of any Operational Service impact:	
Details of any Interfaces affected:	
Reasons for and Benefits and Disadvantages of Requested Contract Change:	
Signature of Requesting Change Owner:	
Date of Request:	

Annex 3 Change
Authorisation Note

CR NO.:	TITLE:	DATE RAISED:
PROJECT:	TYPE OF CHANGE:	REQUIRED BY DATE:
DETAILED DESCRIPTION OF CONTRACT CHANGE FOR WHICH IMPACT ASSESSMENT IS BEING PREPARED AND DETAILS OF ANY RELATED CONTRACT CHANGES:		
PROPOSED ADJUSTMENT TO THE CONTRACT PRICE RESULTING FROM THE CONTRACT CHANGE:		
DETAILS OF PROPOSED ONE-OFF ADDITIONAL CHARGES AND MEANS FOR DETERMINING THESE (E.G. FIXED PRICE OR COST-PLUS BASIS):		
SIGNED ON BEHALF OF AUTHORITY:	SIGNED ON BEHALF OF THE SUPPLIER:	
Signature:_____	Signature:_____	
Name:_____	Name:_____	
Position:_____	Position:_____	
Date:_____	Date:_____	

Addendum 6 – Information Security Questionnaire

Background Information:	Guidance *As a minimum responses should cover the areas below*	Response	Supporting Comments *Provide further detail in support of response and where supporting evidence has been requested, please state the document name provided and relevant section.*
Please describe the service you will be providing to the Authority.	*Summary of service to be provided to the Authority*	Services being provided as per Device Services and Request Services contract, DWP ref 23988	
What type of equipment will be used for the service?		Use of Supplier equipment	
Who will be responsible for managing access to systems in support of the service?		Fully managed by the supplier	
Locations from which the service, including support, will be delivered from, including the access, processing and storage?	*Confirm locations from which the service, including support, will be delivered from, including the access, processing and storage in the 'Supporting Comments' column.* *Provide further detail 'Supporting Comments' column regarding any planned off-shoring.* *The Authority Assets must not be accessed, processed, transmitted and/or stored outside of the United Kingdom without the prior written consent of the Authority and must at all times comply with Data Protection Legislation.* *Offshoring Definition:* *DWP conform to the Cabinet Office definition of offshoring as:* *"Any arrangement where the performance of any part of the service or a solution under contract may occur outside the UK for domestic (UK) consumption".* *This includes:* *●Data hosted outside the UK.* *●Data hosted within the UK but with the potential for access to data from outside the UK.* *●Data temporarily made available offshore for support or diagnostic purposes (Breakfix)* *●Data used for design, build and development activities undertaken outside the UK, including, but not limited to, software code, project management information and solution designs.* *●Foreign nationals brought to the UK for the purpose of fulfilling a central government contract (Landed Resources)*	Within the United Kingdom - Onshore	
What type of access will you require to support the contract?	*Privileged Users are accounts for those that require elevated access rights.* *Please provide details relating to your privileged user requirements in the 'Supporting Comments' column.*	Privileged users with system or service privileges (those with extensive access rights)	
Where will the supplier's personnel, sub-contractors and/or third parties be working from?		Supplier, Sub-contractor and/or Third Party Premises	
Will there be a connection between supplier's, sub-contractor's and/or third parties' networks to the Authority network?	*Provide a description of the proposed connection between supplier's, sub-contractor's and/or third parties' networks to the Authority network.*	No	
Will the service involve the use of subcontractors and/or third parties?	*Please provide details of any subcontractors or third-parties that will support contract delivery, including access, processing, storage or transmission.* *Please confirm the services they will be providing and what they will have access to.*	Yes	Yes, Subcontractors are as follows: Cameo - Break-fix of Microsoft Surface devices Tier 1 - Disposal of Assets Rico Logistics - Secure courier
Will the service be providing software development support to the Authority?	*Security is most effective if planned and managed throughout every stage of software development life cycles (SDLC).* *Please describe the intended software development support to be provided to the Authority.*	No	
Will this service be cloud based?		No	
Will your organisation hold an accreditation or certification to Cloud Security Alliance (CSA) STAR that covers the scope of the service by contract go -live?	*Evidence required will include; a valid STAR certificate provided by a duly CSA accredited provider.*	Please select an answer	
If the service or solution involves card payments, directly or indirectly; will your organisation hold an accreditation or certification to Payment Card Industry Data Security Standards (PCI DSS) that covers the scope of the service by contract go -live?	*Evidence required will include; a valid and appropriate Self Assessment Questionnaires, Report of Compliance and/* *or Attestation of Compliance certificates (based on the volume of card transactions) and duly signed by PCI accredited Qualified Security Assessor (QSA).*	N/A	
Will your organisation hold an accreditation or certification to the current ISO27001 standard that covers the scope of the service by contract go -live?	*Evidence required will include; a valid certificate including scope statement, Statement of Applicability (SoA) and Auditor's report issued by duly accredited provider.*	Yes - ISO27001 certified	
Will your organisation hold an accreditation or certification to Service Organisation Control (SOC) assurance that covers the scope of the service by contract go -live?	*Evidence required will include; an up to date SOC report prepared and signed by a duly accredited independent auditor and a Bridge Letter duly signed by the supplier delegation of authority (if applicable).* *Alternatively an internal audit report which covers the same content as a SOC2 Type 2.*	No	
Will your organisation hold an accreditation or certification to Cyber Essentials or Cyber Essentials Plus that covers the scope of the service by contract go -live?	*Evidence required will include; a valid certificate and scope of certification provided by an NCSC duly accredited provider.*	Yes - Cyber Essentials	CDW are working towards Cyber Essentials Plus
Will your organisation sign up to be a member of Cybersecurity Information Sharing Partnership (CiSP) by contract go -live?	*Evidence required will include; membership number and/or valid certificate provided by National Cyber Security Centre (NCSC).*	Yes	We are members of CiSP. We were not provided any membership numbers or certificates. Further membership requests have been submitted.

Domain	Ref	Question	Guidance *As a minimum responses should cover the requirements detailed below*	*Guidance Hyperlink*	Response	Supporting Comments *How **WILL YOU** meet these requirements?*	Supporting Evidence *Where supporting evidence has been requested/provided, please state the document name provided and relevant section*
Access Control	S01	Will you have a documented User Account Management process in support of the service or solution?	*a) Process should include requirements for joiners, movers and leavers* *b) Identifying users using unique User IDs* *c) Authenticating users using passwords, tokens (smartcards) etc. or biometrics)* *d) Limiting access to those directly involved in the provision of the services and* *e) Granting access on a need to know basis i.e. accessing only the minimum amount of data* *f) Only providing access to applications, computers and networks to fulfil their role* *g) Perform user account and privileged rights reviews periodically which include recertification (is the account still needed) and revalidation (is the access level provided appropriate)* *h) Access and Authentication Controls*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implementated a company wide Information Security Management System (ISMS) that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	Our QMS certifications are audited internal (throughout the year) and external (annually). In accordance with ISO 27001:2013, 5.2 Information Security Policy, specifically Annex A Controls - CDW meets the objective of Annex A.9, Access Control in particular 9.1 to limit access to information and information processing facilities, and 9.2 controls to ensure users are authorised to access systems and services as well as prevent unauthorised access. User Account Management is documented in our policies, processes and procedures to meet the ISO 27001:2013 objectives including: A.9.2.1 User Registration and Deregistration; A.9.2.2 User Access Provisioning; A.9.2.3 Management of Privileged Access Rights; A.9.2.4 Management of Secret Authentication Information of Users; A.9.2.5 Review of User Access Rights; A.9.2.6 Removal or Adjustment of Access Rights to prevent unauthorised access to systems and applications. A.9.4 controls to prevent unauthorised access to systems and applications.
	S02	Will the service or solution include the use of standard or privileged shared accounts?	*a) All Staff (and Sub-Contractor if applicable) must be allocated a unique identifier for their personal and sole use* *b) Generic or shared accounts must not be used to carry out any activities which may be achieved using other individually assigned privileged accounts* *c) All generic or shared account accesses must be subject to a technical risk assessment and authorised in writing by an appropriate Risk Owner or be directly associated with a planned activity* *d) While all account usage is subject to monitoring, the use of generic or shared accounts must not only be monitored, but must always be subject to audit*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implementated a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	Our ISMS ensures compliance with DWP Information Security policy, Security policy, and User Access Control policy. In accordance with ISO 27001:2013, 5.2 Information Security Policy, specifically Annex A Controls - A.9.2.1 User Registration and Deregistration: a) A unique account and password combination authenticate all users of information systems for individual use. The password is retained by, and only known to that individual for all Staff (and Sub-Contractor if applicable). b) We limit shared access IDs. Generic or shared accounts are not used to carry out any activities which may be achieved using other individually assigned privileged accounts. c) Shared access IDs are approved and recorded where utlised in accordance with A.9.2.2 User Access Provisioning. All generic or shared account accesses are subject to a technical risk assessment and authorised in writing by an appropriate Risk Owner or be directly associated with a planned activity. d) Account usage is subject to monitoring. In accordance with A.9.2.5 Review of User Access Rights, periodic reviews are undertaken by the information
	S03	Will you ensure privileged users are restricted and controlled throughout the delivery of a service or solution?	*a) Special access privileges should be documented and given to a limited number of individuals* *b) All Privileged Users must be managed using identity and access management policies* *c) Administrative accounts should only be used to perform legitimate administrative activities, and should not be granted access to email or the internet* *d) There must be a formal authorisation process to grant, assign and approve the allocation of a Privileged User role* *e) Privileged access is only used and granted when it is needed (i.e. when the privileged operation needs to occur) and revoked when it is no longer required* *f) Privileged User access rights must be monitored, reviewed and revalidated periodically to confirm that the levels of access are still required for the role* *g) Segregate privileged access from standard user access on your systems* *h) The use of two-Factor Authentication (2FA)* *i) Privileged users with significant Critical National Infrastructure system or service privileges must have a minimum of Security Check (SC) clearance*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implementated a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	Our ISMS ensures compliance with DWP Information Security policy and in particular Privileged Users Security policy. In accordance with ISO 27001:2013, 5.2 Information Security Policy, specifically Annex A Controls - A.9.2.3 Management of Privileged Access Rights: a) Special access privileges are documented and issued to a limited number of individuals with a formal authorisation processes, also in accordance with A.9.2.2 User Access Provisioning. b) All Privileged Users are managed using identity and access management policies in accordance with A.9.4.1 Information Access Restriction, Role-based access control (RBAC) and Levels of access. c) Administrative accounts are only used to perform legitimate administrative activities, and are not be granted access to email or the internet. We separate the systems administrator role from the day to day user role, these users have two separate accounts. This adheres to the Cyber Essentials: Access Control & Administrative Privilege Management requirement to 'use administrative accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative

Asset Management	S04	Will your Data / Information Classification procedures comply with the HMG Government Security Classifications (GSC)?	*a) Secure labelling* *b) Handling* *c) Transfer* *d) Archiving* *e) Disposal of assets*	https://www.gov.uk/government/publications/government-security-classifications https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implementated a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	Our ISMS ensures compliance with DWP Information Security policy, Security policy, Physical Security policy, Security Classification policy and the Government Security Classifications May 2018. In accordance with ISO 27001:2013, 5.2 Information Security Policy, specifically Annex A Controls – A.8 Asset management. The controls detail the lifecycle of the Data / Information including creation (secure labelling in accordance with A.8.2.2 Labelling of Information); processing (handling - A.8.2.3 Handling of Assets), storage (archiving - A.11.2.1 Equipment Siting & Protection), transmission (transfer - A.13.2.1 Information Transfer Policies & Procedures and A.8.3.3 Physical Media Transfer), deletion and destruction (disposal of assets - A.8.3.2 Disposal of Media) stages. The CDW 'Information Control, Classification & Clear Desk Policy v7.0' and 'Document Control & Records Management Policy' governs classified or sensitive Data / Information. These have recently been updated to reflect HSCN (NHS) data and are in the process of being enhanced to specifically include and Annex for Government Security Classifications.
	S05	Will you have security information transfer agreements for the secure transfer of Authority data between your organisation and external parties used in support of this service or solution?	*a) An agreement document will be signed by both parties that covers this control, and will be available on request* *b) If applicable, provide details on how you plan to transfer Authority data to and from your organisation and external parties*		Yes - we already have this.	CDW has implementated a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	We will have security information transfer agreements implemented for the secure transfer of Authority data between CDW and external parties used in support of this contract. Our ISMS ensures compliance and in accordance with ISO 27001:2013, Annex A.13.2, we maintain the security of information transferred within CDW and with any external entity e.g a customer, supplier or other interested party. The agreement document will be established and signed by both parties in accordance with A.13.2.1 Information Transfer Policies & Procedures and A.13.2.2 Agreements on Information Transfer. In preparation for any transfer plans, our policies, procedures and technical controls will be used to understand the security risks involved in relation to the confidentiality, integrity and availability of information being transferred, with consideration to type, nature, amount and sensitivity or classification.
	S06	Will you have Data Encryption procedures in support of the service or solution?	*a) Internal and external communication channels* *b) Encrypt all data at rest (including local and cloud storage) - with National Cyber Security Centre Commercial (NCSC) Product Assurance (CPA) certification, FIPS 140-2 certification, or National Institute of Standards and Technology (NIST) SP 800-90 certification* *c) Encrypt all data in transit and, where applicable for payment transactions, encryption of all data in process - At the application layer, using Transport Layer Security (TLS); At the network layer, using Internet Protocol Security (IPsec)* *d) Asymmetric private keys and symmetric keys must be stored in location(s) where the principle of least privilege is used to grant or deny access to those key(s)* *e) Backed-up and escrowed keys must be protected to at least the same level as the operational key* *f) In the event of key compromise or suspected key compromise, all authorisations associated with those affected key(s) must be immediately revoked; unless a key compromise recovery plan has identified that availability is more important than confidentiality and integrity, in which case the key compromise recovery plan must be followed*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implementated a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	Our ISMS ensures compliance with DWP Information Security policy. CDW Data Encryption procedures are in accordance with ISO 27001:2013, Annex A.10.1.1 Policy on the use of Cryptographic Controls. The technical controls implemented, including the use of cryptography, protect the confidentiality, authenticity and/or integrity of information. A.10.1.2 Key Management describes the lifecycle from creation, deployment, backup and destruction. The handling, access to, or processing digital certificates and other key material is not currently in the scope of the contract. CDW will provide security measures and safeguards appropriate to the nature and use of the DWP information, where applicable.
	S07	Will a process be in place for handling the return of supplier assets upon termination of employment, contract or agreement?	*Documented process or procedure the organisation follows on recording the return of assets upon termination of employment, contract or agreement.*		Yes - we already have this.	CDW has implementated a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System	Our ISMS ensures compliance with DWP Information Security policy and in particular Personnel Security. In accordance with ISO 27001:2013, handling the return of supplier assets upon termination of employment,
	S08	Will all data be securely deleted or destroyed upon contract termination, expiration or upon Authority request?	*a) Removing and erasing any hidden areas on the Hard Disk Drive (HDD) as part of the erasure process in those cases* *b) Verifying erasure, whether at the end of the process or after each overwriting round to ensure that data sanitization has occurred and to comply with most data erasure standards* *c) Use of NCSC Approved secure deletion tool*	https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media https://www.ncsc.gov.uk/section/products-services/all-products-services-categories?productType=Data%20sanitisation&start=0&rows=20	Yes - we already have this.	CDW has implementated a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	Our ISMS ensures compliance with DWP Information Security policy and Security policy. In accordance with ISO 27001:2013, Annex A.8: Asset Management, specifically A.8.3.2 Disposal of Media. All data be securely deleted or destroyed upon contract termination, expiration or upon Authority request. The CDW 'Information Control, Classification & Clear Desk Policy v7.0' includes section 3.2 Disposal of Confidential Information. CDW has a long-standing relationship and commercial engagement with Tier 1 Asset Management Ltd for the destruction of assets in accordance with HMG Infosec Standard 5 or Contract Authority specific. Tier 1 are NCSC certified, CAS – Sanitisation and members of ADISA (Distinction with Honours). The policies and procedures include the use of NCSC products certified against the Commercial Product Assurance (CPA) scheme. CPA products are evaluated against the Overwriting Tools for Magnetic Media v2.2 Security Characteristic ensuring removal and erasure of hidden areas of storage media and post erasure verification.

Business Continuity / Disaster Recovery	S09	Will you have a documented Business Continuity (BC) Policy and Plan that are reviewed and tested periodically that covers the service or solution?	*Senior Management must be involved with all stages of processes, tests and activities to document a BC Plan to include how the organisation:* *a) Plans business continuity* *b) Implements business continuity* *c) Verifies, tests, reviews and evaluates (lessons learned) business continuity*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.17 Information security aspects of business continuity management ensures we have documented Business Continuity (BC) and Disaster Recovery (DR) Policies. The CDW Business Continuity Plans (BCP) have 3 primary objectives: 1. Define the business dependencies; 2. Business Impact Assessment (BIA) and 3. Modular Plans. These build upon the controls defined in A.17.1.1 Planning Information Security Continuity and A.17.1.2 Implementing Information Security Continuity. Our BCP also incorporates controls defined in A.17.1.3 Verify, Review & Evaluate Information Security Continuity to ensure they are maintained against changes in the business, technologies, and risk levels. We have documented records of internal audits, IS risk assessments including: risk registers and senior management review meeting minutes. Copies of the Strategic RAID Log, Operations Leadership RAID Log and Services Risk Register are also extant. We undertake BC/DR exercises, the most recent undertaken 16/01/2021 where we simulated a complete loss of power in our National Distribution Centre. This was comprehensively reviewed, and lessons learned. Desktop exercises were also
	S10	Will you have a documented Disaster Recovery (DR) Policy and Plan that will be reviewed and tested periodically that covers the service or solution?	*Senior Management must be involved with all stages of processes, tests and activities to document a DR Plan to include how the organisation:* *a) Plans disaster recovery* *b) Implements disaster recovery* *c) Verifies, tests, reviews and evaluates (lessons learned) disaster recovery*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.17 Information security aspects of business continuity management ensures we have documented Business Continuity (BC) and Disaster Recovery (DR) Policies. The CDW Business Continuity Plans (BCP) have 3 primary objectives: 1. Define the business dependencies; 2. Business Impact Assessment (BIA) and 3. Modular Plans. These build upon the controls defined in A.17.1.1 Planning Information Security Continuity and A.17.1.2 Implementing Information Security Continuity. Our BCP also incorporates controls defined in A.17.1.3 Verify, Review & Evaluate Information Security Continuity to ensure they are maintained against changes in the business, technologies, and risk levels. We have documented records of internal audits, IS risk assessments including: risk registers and senior management review meeting minutes. Copies of the Strategic RAID Log, Operations Leadership RAID Log and Services Risk Register are also extant. We undertake BC/DR exercises, the most recent undertaken 16/01/2021 where we simulated a complete loss of power in our National Distribution Centre. This was comprehensively reviewed, and lessons learned. Desktop exercises were also
	S11	Will you have a documented Business Impact Assessment/Analysis (BIA) which determines the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the continuity of the business and service or solution in adverse situations?	*a) BIA document or equivalent outlining business processes and systems* *b) RTO & RPO for all business processes and systems should be captured*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.17 Information security aspects of business continuity management ensures we have documented Business Continuity (BC) and Disaster Recovery (DR) Policies. The CDW Business Continuity Plans (BCP) have 3 primary objectives: 1. Define the business dependencies; 2. Business Impact Assessment (BIA) and 3. Modular Plans. These build upon the controls defined in A.17.1.1 Planning Information Security Continuity and A.17.1.2 Implementing Information Security Continuity. The BIA defines Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for business processes and systems.
	S12	Will you have a Capacity Management process in support of the service or solution?	*a) How system performance will be maintained*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System	In accordance with ISO 27001:2013, Annex A.12 Operational Procedures and Responsibilities, our ISMS ensures compliance.
	S13	Will you have data and network Backup procedures in support of the service or solution?	*a) Backup of information, software, system images* *b) The backups should be stored in a remote location, at a sufficient distance to escape any damage from disaster at the main site* *c) Backup information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site* *d) In situations where confidentiality is of importance, backups should be protected by means of encryption* *e) Periodic testing, reviews and audit*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.12 Operational Procedures and Responsibilities, our ISMS and associated policies ensures compliance. We have documented data and network backup procedures, as defined in control A.12.3.1 Information Backup, in support of CDW services and solutions. This control forms the basis for our 'Backup & Restore Policy' CPOL-IS014 v4.0 and 'ServiceWorks Backup & Restore' v1.0. These include the minimum DWP
Cloud Security	S14	Will there be security controls in place to secure data stored, processed and transmitted in the cloud (private, public and Hybrid)?	*a) Data in transit protection* *b) Asset protection and resilience* *c) Separation between users* *d) Supply chain security* *e) Secure user management* *f) Identity and authentication* *g) Secure use of the service*	https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-cloud-security/principles			
Device Security	S15	Will your service or solution operate a Bring Your Own Device (BYOD) policy?	*The Authority operates a strict zero tolerance relating to BYOD in relation to it's solutions and services.*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System	CDW will not operate any Bring Your Own Device (BYOD) aspects in relation to the core delivery of DWP solutions and services. CDW does have a BYOD policy for the use of particular applications the broader
	S16	Will you have enforce Device Security in support of the service or solution?	*a) Devices must be owned, configured and managed by the Authority or its supplier* *b) Device must be allocated to a named individual for their use only* *c) Users must be provided with guidance on the secure use of mobile devices and remote working* *d) Design principles for any Authority mobile device solution, must follow the NCSC walled garden pattern approach, unless a different approach is approved by the Authority* *e) A user must authenticate to the device using a passcode containing the minimum of six characters, with at least one special character and one capital letter* *f) After 2 minutes of inactivity the device must automatically lock* *g) All usable storage on the device must be encrypted* *h) The data contained on the device must be able to be remotely wiped in the event the device is lost or stolen* *i) Anti-malware must be installed on all devices* *j) A user must not be able to modify or disable security safe guards* *k) Devices must be wiped and all data removed before the device is re-issued to a new user*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.6 Organisation of Information Security, our ISMS and associated policies and Cyber Essentials certification ensures compliance. CDW does enforce device security and will do in support of the service and solutions it provides DWP. Control A.6.2.1 Mobile Device Policy forms the basis for the CDW 'Mobile Device Policy' v3.0 and 'Logical Access Control' CPOL-IS011 v7.0. Devices used to support the DWP contract (a) will be owned by CDW, (b) allocated to a specific individual for sole use, (c) users are provided training and guidance for the secure operation of IT including mobile devices and remote working, (d) CDW will not be delivering any Authority mobile device solution- should there be a requirement, we will follow the NCSC walled garden pattern approach, (e) user authenticate to devices using a passcode which contains a minimum of eight characters, mix of alpha and numeric, at least one digit, a special character and one capital letter, (f) users are reminded to lock their device prior to being unattended with the system auto locking after 2 minutes of activity, (g) usable storage is encrypted in accordance with CDW 'Encryption Policy' CPOL-IS006 v4.0, (h) devices that are powered on and logged in can be remotely erased devices that are

Information Security	S17	Will all staff, contractors and third parties, sign a confidentiality or Non-Disclosure Agreement (NDA) for the protection of data/information related to the service or solution?	*a) Detail the stage this declaration will be carried out.* *b) Provide agreement here that, where at the written request of the Authority, the Supplier shall obtain individual confidentiality statements from supplier's personnel including subcontractors.*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.13: Communications Security, our ISMS and associated policies and Cyber Essentials certification ensures compliance. CDW ensures all staff, contractors and third parties, sign confidentiality or Non-Disclosure Agreements (NDA) for the protection of CDW and client data/information. Control A.13.2.4 Confidentiality or Non-Disclosure Agreements, forms the basis for Information Security being included in the Contract of Employment offers s.20 (pre commencement of employment), Computer Security s.21, Intellectual Property, Inventions and Copyright and s.24 Data Protection. Where specific clients such as DWP require additional NDA's completing, these will be managed by Co-Worker Services (CWS) and the management team prior to any commencement of work. Non-disclosure agreements are also in place for contractors and temporary personnel based on the CDW 'Non-Disclosure Agreement' v4.0, with employee ongoing obligations managed as part of their conditions of employment and detailed in the 'CDW UK Co-worker Handbook - Road To Success'.
	S18	Will employment contracts include clauses to protect information assets and state all employees' responsibilities for information security?	*Declaration only*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.13: Communications Security, our ISMS and associated policies and Cyber Essentials certification ensures compliance. CDW ensures all staff, contractors and third parties, sign confidentiality or Non-Disclosure Agreements (NDA) for the protection of CDW and client data/information. Control A.13.2.4 Confidentiality or Non-Disclosure Agreements, forms the basis for Information Security being included in the Contract of Employment offers s.20 (pre commencement of employment), Computer Security s.21, Intellectual Property, Inventions and Copyright and s.24 Data Protection stating employees' responsibilities. Ongoing responsibilities are managed as conditions of employment and detailed in the 'CDW UK Co-worker Handbook - Road To Success'.
	S19	Will the configuration of your teams support segregation of duties throughout the delivery of this service or solution?	*a) Segregation of duties to reduce opportunities for unauthorised or unintentional modification or misuse of assets*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, controls are in place to comply with Annex A.6: Organisation of Information Security, in particular A.6.1.1 Information Security Roles & Responsibilities. A.6.1.2 Segregation of Duties to mitigate the opportunity for unauthorised or unintentional modification or misuse of any assets. Our policies and procedures include the configuration of our teams in support of the delivery of the service or solution of this contract. Segregation of duties are also included in the CDW 'Secure Development Policy' v7.0 and ISO 20000:2018 Information technology - Service Management and clause 8.2.5 Asset Management to ensure CDW meets the requirements and obligations.
	S20	Will you have Acceptable Use procedures in support of the service or solution?	*a) All staff, contractors and third parties read and acknowledge their understanding of all security policies, standards and procedures prior to gaining access to data or providing services*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System	In accordance with ISO 27001:2013, Annex A.8: Asset Management, our ISMS and associated policies ensures compliance.
	S21	Will you safeguard voice or video recordings that may be involved in the delivery of the service or solution?	*a) There must be consideration to determine the necessity for technical countermeasures required such as intrusion detection/prevention system* *b) All relevant Voice Over IP (VoIP)/Video communications systems must ensure security is in place to protect against malicious software and to restrict access* *c) All relevant VoIP/Video Communications software/hardware must be maintained with the latest approved patches and current versions*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, we understand the necessity to safeguard all data/information including voice or video recordings. CDW does not envisage voice or video recordings being delivered under the contract. Controls are in place to comply with Annex A.13: Communications Security, in particular A.13.1.2 Security of Network Services and A.13.2.1 Information Transfer Policies & Procedures underpin the CDW 'Encryption Policy' CPOK-IS006 v4.0, including the transmission of data such as VoIP/Video communications. In accordance with Cyber Essentials and other best practice information security frameworks such as 'NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations', CDW ensures suitable technical countermeasures including intrusion detection/prevention systems are operational. CDW policy includes 'Firewall Policy' CPOL-IS004 v2.0, referencing NIST SP 800-41 Rev 1.
	S22	Will you have a process in place to ensure security controls are in place for remote working (teleworking)?	*a) A user must authenticate to the endpoint device using an approved authentication mechanism, such as two factor authentication* *b) The authentication password must comply with NCSC guidelines* *c) Where certificates are used for authentication of device or user, they must comply with NCSC guidelines* *d) Where certificates or private keys are utilised they must be housed in a tamper proof module to prevent unauthorised access, including a Trusted Platform Module (TPM) for laptop whole disk encryption and smart cards for user access control* *e) Where a Virtual Private Network Client is required, it must be installed on all endpoints prior to deployment* *f) Whole disk encryption must be applied to the Device, prior to Authority data being stored on it* *g) Appropriate guidance issued to staff relating to Remote Working security controls*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.6: Organisation of Information Security, our ISMS, associated policies and Cyber Essentials certification ensures compliance. CDW enforces security controls for all employees including remote workers. Control A.6.2.1 Mobile Device Policy forms the basis for the CDW 'Mobile Device Policy' v3.0 and 'Logical Access Control' CPOL-IS011 v7.0. Standard users, using corporate provisioned devices access endpoint devices using (a) username and password credentials, with Citrix environment remote users having additional Signify token generation authentication (two-factor). (b) Passwords comply with NCSC guidelines and the Cyber Essentials 'Password-based authentication' requirements. (c) Where a trusted authority is used (for the purposes of issuing and maintaining digital signatures or certificates) security is integrated and embedded throughout the entire end-to-end certificates as per the CDW 'Application Services on Public Networks Policy' v2.0. (d/f) Where certificates or private keys are used, controls are implemented to prevent unauthorised access including the use of TPM for whole disk encryption utilising Microsoft Bitlocker in accordance with CDW 'Encryption Policy' CPOL-IS006 v4.0 and
	S23	In relation to the service or solution, will you perform Baseline Personnel Security Standard (BPSS) security checks for all staff, contractors and third parties prior to granting access to Authority data?	*The BPSS comprises verification of the following four main elements;* *• Identity* *• Nationality and Immigration Status (including an entitlement to undertake the work in question)* *• Employment history (past 3 years)* *• Criminal record (unspent convictions only*	https://www.gov.uk/government/publications/government-baseline-personnel-security-standard	Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	Our ISMS ensures compliance with DWP Personnel Security policy. In accordance with ISO 27001:2013, Annex A Controls – A.7 Human resource security, specifically A.7.1.1 Screening covering background verification and competence checks for all employees, contractors and third parties prior to granting access to Authority data. Employment screening is used and where necessary and proportionate, National Security Vetting is also used. The CDW Co-Worker Services (CWS) team manage all aspects of HR, personnel security, and recruitment checks. This includes pre-employment screening, the management of BPSS, DBS checks, any subsequent Security Clearance applications including aftercare obligations. BPSS is a pre-requisite for Security Clearance.
	S24	For enhanced positions, will you engage with the Authority to perform enhanced security vetting before access is granted to sensitive information?	*Declaration only*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	We will work with the Authority to perform enhanced security vetting before access is granted to sensitive information. CDW works with United Kingdom Security Vetting (UKSV) as its provider of National Security Vetting
	S25	Will you have a documented disciplinary and grievance process for handling activities against security policies and standards?	Declaration only		Yes - we already have this.		

Legal and Compliance	S26	Will you regularly review and audit compliance with regulations, policies and standards (including monitoring compliance to Data Protection Legislation)?	*Declaration only*		Yes - we already have this.		
Network Security	S27	Will you have Network Security procedures in relation to the delivery of the service or solution?	*a) Periodic reviews* *b) Use of firewalls; including device hardening and regularity of ruleset checks* *c) Use of Host-based Intrusion Detection System (HIDS)/Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), Network Intrusion Detection System, Security Information and Event Management* *d) Use of controls mitigating Distributed Denial Of Service (DDOS) risks* *e) Type of encrypted wireless connection used* *f) Segregation between business and guest traffic* *g) Segregation between test and production environments* *h) Periodic tests of all segregation controls* *i) The use of passive/active Wireless Local Area Network (WLAN) scanners* *j) Penetration testing is performed periodically or after significant network changes with the view of taking appropriate measures to address associated risks* *k) Internal and external vulnerability scanning is performed periodically on your environment with a view of taking appropriate measures to address associated risk*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.13: Communications Security and 13.1.1 Network Controls, CDW networks are managed and controlled and audited periodically to protect information within systems and applications including adherence to controls defined in A.13.1.2 Security of Network Services. (a,b,c,d) CDW policy includes 'Firewall Policy' CPOL-IS004 v2.0, referencing NIST SP 800-41 Rev 1. All configuration meets the Cyber Essentials technical controls for firewalls and secure configuration which includes provision for HIDS, IDS, IPS, Network Intrusion Detection System, SIEM and DDOS mitigation controls. (e,f,g) CDW has encrypted wireless connectivity for corporate use, locked to corporate issued devices. Guest wireless access is also provided, with all traffic / user types segregated including between test and production environments. The CDW 'Configuration Centre Network Access Policy' v1.0 also provides access controls implemented. (h,j,k) Penetration testing is performed annually or after significant network changes in accordance with PCI DSS and Cyber Essentials, included in CDW
	S28	In relation to the service or solution, will you have secure Firewall configurations and procedures?	*a) One or more firewalls (or equivalent network device) should be installed on the boundary of the organisation's internal network(s) and segregating sensitive environments (e.g. Card Holder Data Environment (CDE))* *b) The default administrative password for any firewall (or equivalent network device) should be changed to an alternative, strong password* *c) Each rule that allows network traffic to pass through the firewall requires approval by an authorised individual and documented (including an explanation of business need)* *d) Unapproved services, or services that are typically vulnerable to attack (such as Server Message Block (SMB), NetBIOS, tftp, RPC, rlogin, rsh or rexec), should be disabled (blocked) at the boundary firewall by default* *e) Firewall rules that are no longer required should be removed or disabled in a timely manner* *f) The administrative interface used to manage boundary firewall*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.13: Communications Security and 13.1.1 Network Controls, CDW networks are managed and controlled and audited periodically to protect information within systems and applications including adherence to controls defined in A.13.1.2 Security of Network Services. CDW policy includes 'Firewall Policy' CPOL-IS004 v2.0, referencing NIST SP 800-41 Rev 1. All configuration meets the Cyber Essentials technical controls for firewalls and secure configuration. Firewalls are installed and operational on the boundary of the CDW internal networks, with sensitive environments segregated. All default administrative passwords are changed to a strong password. The
	S29	Will you ensure all changes to all applications and systems are tested and approved prior to implementation or deployment to the production environment?	*A formal change management process to ensure changes made are recorded, tested and approved before being implemented.*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.12 Operational Procedures and Responsibilities, our ISMS ensures compliance with the implemented controls under Annex A.12.1.2 Change Management and A.12.1.4 Separation of Development, Testing & Operational Environments. The CDW 'IT Service Management' supports our ISO 20000:2018 Information technology - Service Management certification provides an overview of the implemented Integrated Management System to ensure changes to all applications and systems are tested and approved prior to implementation or deployment to production environments. These are further supported by the formal 'Change and Release Management Policy' and 'Change and Release Management Processes'.
	S30	In relation to the service or solution, will you use live (production) Authority data in testing or development environment?	*a) Declaration if any Authority data will be used in the testing or development environment.*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.12 Operational Procedures and Responsibilities, our ISMS ensures compliance with the implemented controls under Annex A.12.1.2 Change Management and A.12.1.4 Separation of Development, Testing & Operational Environments. The CDW 'IT Service Management' supports our ISO 20000:2018 Information technology - Service Management certification provides an overview of the implemented Integrated Management System to ensure changes to all applications and systems are tested and approved prior to implementation or deployment to production environments. These are further supported by the formal 'Change and Release Management Policy' and 'Change and Release Management Processes'.

Physical Security	S31	Will you have physical security measures in place covering offices, rooms, and Information processing facilities?	*a) Carry out physical security audits/reviews periodically* *b) Clear-desk/Clear-screen Policy for papers, removable media and information processing facilities* *c) Physical security controls in place to protect secure areas including visitor access* *d) Controls in place to protect equipment and facilities against natural disasters and other incidents or interruptions, malicious or otherwise* *e) Monitor physical access and review access logs to the facilities to detect and respond to physical security incidents* *f) Controls in place to protect cables carrying data against interception, interference or damage*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.11: Physical & Environmental Security, our ISMS ensures compliance with the implemented controls against A.11.1.1 through to A.11.1.6. We hold Facility Security Clearance (also known as List-x) independently audited by the UK MoD – Principle Security Advice Centre (PSyA) and work in conjunction with local Counter Terrorism Security Advisor (CTSA) team. a) Daily physical security audits/reviews are undertaken with a weekly Security Working Group (SWG), formally recorded. b) CDW has an established 'Information Classification, Control & Clear Desk Policy' in addition to the 'Document Control & Records Management Policy' to meet objectives outlined in 7.5 of ISO 9001, 14001 and 27001 in addition to objectives described in 4.3.2, 4.3.3 in ISO 20000 for documented information and a removable media policy. Training, awareness and ongoing security campaigns are provided. c) Physical security controls are in place to protect secure areas including visitor access. CDW have an extant Physical & Environmental Security Policy. Security Operating Procedures (SOP's) promote attack failure and deny visitors. Visitors are pre-booked only, validated upon arrival by security guards.
Protective Monitoring	S32	In relation to the service or solution, will you produce, retain and regularly review event logs?	*a) Recording of user activities, exceptions, faults and information security events* *b) Physical Security logs retained for 6 months* *c) Successful and failed logon attempt logs retained for 90 days* *d) You shall have an audit trail which can be interrogated by authorised individuals and will identify who has:* *• Performed an action, which means;* *o Browsing information* *o Creating information* *o Updating information* *o Deleting information* *• What they did* *• When they did it* *• Where they did it from*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.12: Operational Procedures and Responsibilities, our ISMS ensures compliance with the implemented controls against A.12.4.1 Event Logging. The controls underpin the CDW 'Information Security Event & Incident Reporting & Management Policy' v14.0, the policy includes procedures that apply to all Events of Interest and Incidents for CDW, whether physical or electronic in nature. CDW Information Security monitor email and internet activity using FireEye EX and FireEye NX. CDW corporate systems: a) Record user activities, exceptions, faults and information security events b) In conjunction with the Security Guards, physical Security logs retained for 6 months c) Logs successful and failed logon attempt logs retained for 90 days d) Provide an audit trail which can be interrogated by authorised individuals and can identify who has performed an action, such as Browsing information, Creating information, Updating information, Deleting information, including what they did, when and where from.
	S33	In relation to the service or solution, will you log and review privileged user activities?	*a) You shall have an audit trail which can be interrogated by authorised individuals and will identify who has:* *• Performed an action, which means;* *o Browsing information* *o Creating information* *o Updating information* *o Deleting information* *• What they did* *• When they did it* *• Where they did it from*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.12: Operational Procedures and Responsibilities, our ISMS ensures compliance with the implemented controls against A.12.4.1 Event Logging. The controls underpin the CDW 'Information Security Event & Incident Reporting & Management Policy' v14.0, the policy includes procedures that apply to all Events of Interest and Incidents for CDW, whether physical or electronic in nature and privileged users in support of A.12.4.3 Administrator & Operator Logs. CDW Information Security monitor email and internet activity using FireEye EX and FireEye NX. CDW corporate systems: a) Record user activities, exceptions, faults and information security events b) In conjunction with the Security Guards, physical Security logs retained for 6 months c) Logs successful and failed logon attempt logs retained for 90 days d) Provide an audit trail which can be interrogated by authorised individuals and can identify who has performed an action, such as Browsing information, Creating information, Updating information, Deleting information, including what they did, when and where from.
	S34	In relation to the service or solution, are there controls in place to protect logging facilities and log information from unauthorised changes?	*a) Ensure logging facilities and log information is protected against tampering and unauthorised access*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards	Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.12: Operational Procedures and Responsibilities, our ISMS ensures compliance with the implemented controls against A.12.4.1 Event Logging. The controls underpin the CDW 'Information Security Event & Incident Reporting & Management Policy' v14.0, the policy includes procedures that apply to all Events of Interest and Incidents for CDW, whether physical or electronic in nature and privileged users in support of A.12.4.2 Protection of Log Information. CDW ensure logging facilities and log information is protected against tampering and unauthorised access.
Secure Development of Software Development	S35	Will your project and development lifecycles include security from the planning/feasibility phase and throughout?	*a) Ensure information security is designed and implemented within the project and development lifecycle of information systems*	https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards			
	S36	Will all of your developers, receive secure coding training periodically?	*a) Developers should be trained in the secure use, testing and review of code*				
	S37	Will you have a process that restricts the access to source/mobile code on a need to know basis?	*a) Access to source/ mobile code should be restricted* *b) Audit log should be maintained of all access to source libraries* *c) Updating, maintenance and copying of source libraries should be subject to strict change control procedures* *d) Held/ stored in a secure environment*				
Supplier Assurance	S38	Will you manage your third-parties and sub-contractors, in support of the service or solution, to ensure they are compliant with the Authority security requirements?	*a) establish and agree all relevant security requirements within contracts for your suppliers that process, store or transmit Authority data.* *b) perform security due diligence and assessment on third parties in your supply chain prior to on-boarding.* *c) monitor, review and audit existing third parties in your supply chain periodically to ensure they maintain an agreed level of security.*		Yes - we already have this.	CDW has implemented a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 - Information Security, Quality Management System (QMS).	In accordance with ISO 27001:2013, Annex A.15: Supplier Relationships, our ISMS ensures compliance with the implemented controls against A.15.1.1 Information Security Policy for Supplier Relationships through to A.15.2.2 Managing Changes to Supplier Services. Third-parties, sub-contractors, including delivery partners, service providers and general suppliers are managed under our Supplier Management Procedure which includes aspects detailed in the 'Mitigating Security Risk in the National Infrastructure Supply Chain' guidance. These procedures include risk assessment, due diligence/accreditation/assurance checks to ensure proportionate and appropriate measures are implemented and managed through audit and compliance regimes. Security Aspect Letters (SALs) and classified guides are managed by the Security Controller (SC). The SC engages with Head of Public Sector Enablement and Supply Chain Management to ensure the requirements are understood and specifics disseminated to the appropriate personnel. Where classified work is sub-contracted, we adhere to the strict 'Contractual Processes' in addition to our