**RM6100 Technology Services 3 Agreement**

**Framework Schedule 4 - Annex 1**

**Lots 2, 3 and 5 Order Form**

Contract Reference: CCSO22A02 / DWP ecm\_10345

TCS BaNCS Application Development and Live Service Support Contract

**Order Form**

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 dated 16th June 2021 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms. The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website <http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm1234>. The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

The Supplier shall provide the Services and/or Goods specified in this Order Form (including any attachments to this Order Form) to the Buyer on and subject to the terms of the Contract for the duration of the Contract Period.

In this Order Form, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) of the Call-Off Terms

This Order Form shall comprise:

1. This document headed “Order Form”;
2. Attachment 1 – Services Specification;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits;
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
7. Attachment 8 - Governance Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
8. Attachment 10 – Transparency Reports;
9. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses; and
10. Attachment 11 – DWP Security Provisions

The Order of Precedence shall be as set out in Clause 2.2 of the Call-Off Terms being:

### the Framework, except Framework Schedule 18 (Tender);

### the Order Form;

### the Call Off Terms; and

### Framework Schedule 18 (Tender).

**Section A**

**General information**

| **Contract Details** | |
| --- | --- |
| **Contract Reference:** | CCSO22A02  DWP – ecm\_10345 |

| **Contract Title:** | TCS BaNCS Application Development & Live Service Support Contract. |
| --- | --- |

| **Contract Description:** | Provision of Application Development & Live Support Services of the TCS BaNCS component of the CMG CMS2012 Application |
| --- | --- |

| **Contract Anticipated Potential Value:** this should set out the total potential value of the Contract | Up to a maximum of £2,400,000.00 including all expenses but excluding VAT. |
| --- | --- |

| **Estimated Year 1 Charges:** | £600,000.00 |
| --- | --- |

| **Commencement Date:** this should be the date of the last signature on Section E of this Order Form | 3rd October 2022 |
| --- | --- |

| **Buyer details** |
| --- |
| **Buyer organisation name**  Department for Work and Pensions |

| **Billing address**  Your organisation’s billing address - please ensure you include a postcode  **REDACTED TEXT under FOIA Section 40, Personal Information**.    [APinvoices-DWP-U@gov.sscl.com](mailto:APinvoices-DWP-U@gov.sscl.com) |
| --- |

| **Buyer representative name**  The name of your point of contact for this Order  **REDACTED TEXT under FOIA Section 40, Personal Information**. |
| --- |

| **Buyer representative contact details**  Email and telephone contact details for the Buyer’s representative. This must include an email for the purpose of Clause 50.6 of the Contract. |
| --- |

| **Buyer Project Reference**  Please provide the customer project reference number.  Project\_24634 / CCSO22A02 |
| --- |

| **Supplier details** |
| --- |
| **Supplier name**  Tata Consultancy Services Limited |

| **Supplier address**  Supplier’s registered address  **REDACTED TEXT under FOIA Section 40, Personal Information**. |
| --- |

| **Supplier representative name**  The name of the Supplier point of contact for this Order  **REDACTED TEXT under FOIA Section 40, Personal Information**. |
| --- |

| **Supplier representative contact details**  Email and telephone contact details of the supplier’s representative. This must include an email for the purpose of Clause 50.6 of the Contract.  **REDACTED TEXT under FOIA Section 40, Personal Information**. |
| --- |

| **Order reference number or the Supplier’s Catalogue Service Offer Reference Number**  CCSO22A02 |
| --- |

| **Guarantor details**  *Guidance Note: Where the additional clause in respect of the guarantee has been selected to apply to this Contract under Part C of this Order Form, include details of the Guarantor immediately below.* |
| --- |
| **Guarantor Company Name**  The guarantor organisation name  N/A |

| **Guarantor Company Number**  Guarantor’s registered company number  N/A |
| --- |

| **Guarantor Registered Address**  Guarantor’s registered address  N/A |
| --- |

**Section B**

**Part A – Framework Lot**

| **Framework Lot under which this Order is being placed** | |
| --- | --- |
| 1. TECHNOLOGY STRATEGY & SERVICES DESIGN | ☐ |
| 1. TRANSITION & TRANSFORMATION | ☐ |
| 1. OPERATIONAL SERVICES |  |
| a: End User Services | ☐ |
| b: Operational Management | ☐ |
| c: Technical Management | ☐ |
| d: Application and Data Management | ☑ |
| 1. SERVICE INTEGRATION AND MANAGEMENT | ☐ |

**Part B – The Services Requirement**

| **Commencement Date**  See above in Section A |
| --- |

| **Contract Period:** The contract will commence on 3rd of October 2022 and operate for an initial 36-month period to 31st August 2025. There is an option to extend the contract for a further 12 months to 31st August 2026. (3 + 1). | | |
| --- | --- | --- |
| **Initial Term** Months  36 | **Extension Period (Optional)** Months  12 | |
| **Minimum Notice Period for exercise of Termination Without Cause**  (Calendar days) Insert *right (see Clause 35.1.9 of the Call-Off Terms)* | | 30 |

| **Sites for the provision of the Services**  The Supplier shall provide the Services from the following Sites**:**  **Buyer Premises:**  **REDACTED TEXT under FOIA Section 40, Personal Information**.  **Supplier Premises:**  N/A  **Third Party Premises:**  N/A |
| --- |

| **Buyer Assets**  *Guidance Note: see definition of Buyer Assets in Schedule 1 of the Call-Off Terms*  The Buyer to provide the following equipment under this Call Off Contract:   1. Access to the Buyer site(s) as required (where necessary and appropriate). 2. Buyer laptops and equipment provided to the supplier and to each of Supplier’s personnel providing the Services in the UK together with email account for the duration of the Call Off Contract. 3. Buyer infrastructure and hosting environments accessed and used by the Supplier in connection with the provision of the Services. 4. All information and relevant documentation provided by the Buyer or produced by the Supplier, relative to the Services that are being provided under this contract. 5. Any software owned by and/or licensed or leased to the Buyer used by the Supplier in connection with the provision of the Services. |
| --- |

| **Additional Standards** The technology code of practice - <https://www.gov.uk/guidance/the-technology-code-of-practice>  * Open Standards principles - <https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles> * Open standards for government data and technology - <https://www.gov.uk/government/collections/open-standards-for-government-data-and-technology> * The Supplier shall produce full and detailed technical architecture documentation for the Supplier solution in accordance with Good Industry Practice. * **Accessible Digital Standards:** The Supplier shall comply with (or with equivalents to):   1. the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.1 Conformance Level AA; and   2. ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability   **SERVICE MANAGEMENT SOFTWARE & STANDARDS**  The Supplier shall reference relevant industry and HM Government standards and best practice guidelines in the management of the Services, including the following and/or their equivalents:   1. ITIL v4; 2. ISO/IEC 20000-1 2018 “Information technology — Service management – Part 1”; 3. ISO/IEC 20000-2 2019 “Information technology — Service management – Part 2”; 4. ISO 10007: 2017 “Quality management systems – Guidelines for configuration management”; and 5. ISO 22313:2020 “Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301” and, ISO/IEC 27031:2011 and ISO 22301:2019.   For the purposes of management of the Services and delivery performance the Supplier shall make use of Software that complies with Good Industry Practice including availability, change, incident, knowledge, problem, release & deployment, request fulfilment, service asset and configuration, service catalogue, service level and service portfolio management. If such Software has been assessed under the ITIL Software Scheme as being compliant to “Bronze Level”, then this shall be deemed acceptable.  **TECHNOLOGY ARCHITECTURE STANDARDS**  The Supplier shall produce full and detailed technical architecture documentation for the Supplier solution in accordance with Good Industry Practice. If documentation exists that complies with the Open Group Architecture Framework 9.2 or its equivalent, then this shall be deemed acceptable. |
| --- |

| **Buyer Security Policy**  The Security Policies are published on:  <https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards> |
| --- |

| **Buyer ICT Policy**  *Guidance Note: where the Supplier is required to comply with the Buyer’s ICT Policy then append to this Order Form below.*  [DWP Acceptable Use Policy (publishing.service.gov.uk)](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/839545/dwp-acceptable-use-policy.pdf) |
| --- |

| **Insurance**  *Guidance Note: if the Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Agreement or the Buyer requires any additional insurances please specify the details below.*  Third Party Public Liability Insurance (£) - £1million  Professional Indemnity Insurance (£) - £1million  UK Employer’s Liability Insurance (£) - £5million |
| --- |

| **Buyer Responsibilities**  *Guidance Note: list any applicable Buyer Responsibilities below.*  The Buyer shall   * perform those obligations which are set out in the clauses of this Contract and the paragraphs of the schedules; * make available the software and procure the supply of the items of hardware and associated services which are necessary to enable the Supplier to perform the Services set out is the Contract. Unless otherwise agreed, the Buyer shall retain ownership of and the Supplier shall retain risk in the assets; * use its reasonable endeavours to provide the Supplier with access to appropriate members of the Buyer’s staff, as such access is reasonably requested by the Supplier in order for the Supplier to discharge its obligations throughout the Term; * ensure that all project risks, assumptions, issues and dependencies including 3rd party supplier and product vendor dependencies have been addressed within planned timelines; * provide sufficient and suitably qualified staff to fulfil the Buyer’s roles and duties under this Contract, in particular to work with the Supplier to:   + agree the scope of each sprint;   + agree and sign off agreed deliverables in respect of the acceptance criteria in good time such that the sign off does not impact deployment; * use its reasonable endeavours to provide such documentation, data and/or other information that the Supplier reasonably requests that is necessary to perform its obligations under the terms of this Contract provided that such documentation, data and/or information is available to the Buyer and is authorised for release by the Buyer. * procure for the Supplier such agreed access and use of the Buyer’s premises, facilities, including relevant ICT systems as is reasonably required for the Supplier to comply with its obligations under this Contract, such access to be provided during the Buyer's normal working hours on each Working Day or otherwise as agreed by the Buyer (such agreement not to be unreasonably withheld or delayed). |
| --- |
|  |

| **Goods**  Not Applicable |
| --- |

| **Governance – Option Part A or Part B**  *Guidance Note: The Call-Off Terms has two options in respect of governance. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is limited project governance required during the Contract Period.*   | **Governance Schedule** | **Tick as applicable** | | --- | --- | | Part A – Short Form Governance Schedule | ☑☐ | | Part B – Long Form Governance Schedule |  |   The Part selected above shall apply this Contract. |
| --- | --- | --- | --- | --- | --- | --- |

| **Change Control Procedure – Option Part A or Part B**  *Guidance Note: The Call-Off Terms has two options in respect of change control. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is no requirement to include a complex change control procedure where operational and fast track changes will not be required.*   | **Change Control Schedule** | **Tick as applicable** | | --- | --- | | Part A – Short Form Change Control Schedule | ☐ | | Part B – Long Form Change Control Schedule | ☑ |   The Part selected above shall apply this Contract. Where Part B is selected, the following information shall be incorporated into Part B of Schedule 5 (Change Control Procedure):   * for the purpose of Paragraph 3.1.2 (a), the figure shall be £5,000.00 in aggregate in any one calendar month; and * for the purpose of Paragraph 8.2.2, the figure shall be £50,000.00. |
| --- | --- | --- | --- | --- | --- | --- |

**Section C**

**Part A - Additional and Alternative Buyer Terms**

| **Additional Schedules and Clauses** *(see Annex 3 of Framework Schedule 4)*  *This Annex can be found on the RM6100 CCS webpage. The document is titled RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5.*  **Part A – Additional Schedules**  *Guidance Note: Tick any applicable boxes below*   | **Additional Schedules** | **Tick as applicable** | | --- | --- | | S1: Implementation Plan | ☑ | | S2: Testing Procedures | ☑ | | S3: Security Requirements (either Part A or Part B) | Part A ☐ or Part B ☑ | | S4: Staff Transfer | ☐ N/A | | S5: Benchmarking | ☐ N/A | | S6: Business Continuity and Disaster Recovery | ☑ | | S7: Continuous Improvement | ☑ | | S8: Guarantee | ☐ N/A | | S9: MOD Terms | ☐ N/A |   **Part B – Additional Clauses**  *Guidance Note: Tick any applicable boxes below*   | **Additional Clauses** | **Tick as applicable** | | --- | --- | | C1: Relevant Convictions | ☐ N/A | | C2: Security Measures | N/A | | C3: Collaboration Agreement | ☐N/A |   Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.  **Part C - Alternative Clauses**  The following Alternative Clauses will apply:   | **Alternative Clauses** | **Tick as applicable** | | --- | --- | | Scots Law | ☐ N/A | | Northern Ireland Law | ☐ N/A | | Joint Controller Clauses | ☐ N/A |   Where selected above the Alternative Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract. |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

**Part B - Additional Information Required for Additional Schedules/Clauses Selected in Part A**

| **Additional Schedule S3 (Security Requirements)**  *Guidance Note: where Schedule S3 (Security Requirements) has been selected in Part A of Section C above, then for the purpose of the definition of “Security Management Plan” insert the Supplier’s draft security management plan below.*  *If applicable, Supplier need to insert their “Security Management Plan” here.* |
| --- |

| **Additional Schedule S4 (Staff Transfer)**  *Guidance Note: where Schedule S4 (Staff Transfer) has been selected in Part A of Section C above, then for the purpose of the definition of “Fund” in Annex D2 (LGPS) of Part D (Pension) insert details of the applicable fund below.*  Not Applicable |
| --- |

| **Additional Clause C1 (Relevant Convictions)**  Not Applicable |
| --- |

| **Additional Clause C3 (Collaboration Agreement)**  *Guidance Note: where Clause C3 (Collaboration Agreement) has been selected in Part A of Section C above, include details of organisation(s) required to collaborate immediately below.*  Not Applicable |
| --- |

**Section D**

**Supplier Response**

| **Commercially Sensitive information**  Any confidential information that the Supplier considers sensitive for the duration of an awarded Contract should be included here. Please refer to definition of Commercially Sensitive Information in the Contract – *use specific references to sections rather than copying the relevant information here.*  TBC |
| --- |

**Section E**

**Contract Award**

This Call Off Contract is awarded in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100.

| **SIGNATURES** |
| --- |

**For and on behalf of the Supplier**

| Name | **REDACTED TEXT under FOIA Section 40, Personal Information.** |
| --- | --- |
| Job role/title | **REDACTED TEXT under FOIA Section 40, Personal Information.** |
| Signature | **REDACTED TEXT under FOIA Section 40, Personal Information.** |
| Date |  |

**For and on behalf of the Buyer**

| Name | **REDACTED TEXT under FOIA Section 40, Personal Information.** |
| --- | --- |
| Job role/title | **REDACTED TEXT under FOIA Section 40, Personal Information.** |
| Signature | **REDACTED TEXT under FOIA Section 40, Personal Information.** |
| Date |  |

**Attachment 1 – Services Specification**

# PURPOSE

## The Department for Work and Pensions is re-procuring the services to provide Application Development and Live Service Support services for TCS BaNCS, which is a core component of the DWP CMS 2012 System.

# BACKGROUND TO THE CONTRACTING authority

## The Department for Work and Pensions (DWP) is responsible for welfare, pensions and child maintenance policy. As the UK’s biggest public service department, it administers the State Pension and a range of working age, disability and ill health benefits to around 20 million claimants and customers.

## We provide our services in a number of ways, for example through Jobcentre Plus, The Pension Service, the Child Maintenance Service and partner organisations.

## This requirement is in support of the Child Maintenance Group (CMG). The overall objective of the Child Maintenance Group is ‘to maximise the number of those children who live apart from one or both parents for whom effective child maintenance arrangements are in place’.

## Our vision is: 'Helping to Improve Children's Lives'. We deliver our vision by:

## Promoting the financial responsibility that parents have for their children.

## Providing Information and support about the different child maintenance options that are available and supporting families in making their own family-based arrangements.

## Delivering an efficient statutory maintenance service, with effective enforcement support.

## We want to create a future where it is the norm for separated parents to support their children financially.

## Further information can be found on-line at [About us - Department for Work and Pensions - GOV.UK (www.gov.uk)](https://www.gov.uk/government/organisations/department-for-work-pensions/about)

# Background to requirement/OVERVIEW of requirement

## CMG is responsible for the administration of the Child Maintenance Service. CMG relies on the Child Maintenance Service 2012 Scheme system (CMS 2012), along with other systems, to deliver its services to customers.

## The current contract with the incumbent Supplier that provides application development and live support services for TCS BaNCS is due to shortly expire. The incumbent has been providing such services to DWP under various contractual arrangements since 2009.

## A Supplier is required to provide capacity and capability to support DWP to deliver outcomes in the areas of development, change and repair across a series of releases, and live support necessary to satisfy the requirements for a stable performance application.

## TCS BaNCS is a core component of the CMS 2012 System which is a highly integrated solution comprising of several COTS packages, that supports CMG operational delivery to serve its customers. TCS BaNCS has been customised by the incumbent Supplier to meet CMG’s specific requirements and is critical to CMG business practices.

## It is anticipated by the end of March 2025 that TCS BaNCS will be replaced by a common shared component delivered by DWP’s Application Reference Architecture (ARA) strategy.

## Other key technologies of the CMS 2012 System, in addition to having an in-depth knowledge of the TCS BaNCS product, the Supplier would be expected to have experience in Siebel and BPM.

## The functionality of the TCS BaNCS software supports the following:

* Processing of daily transactions.
* Set up and management of client accounts.
* Processing and posting of payment receipts to appropriate accounts.
* Suspense account management.
* Allocation of payments.
* Generating outbound and managing inbound payments.
* Assigning payments to receiving parents' account.
* Missed payments and arrears tracking.
* Posting of information to general Ledger.
* Management of liability and postings schedules.
* Management of refunds, adjustments, and manual payment processing.
* Statement and schedule generation.

# definitions

| Expression or Acronym | **Definition** |
| --- | --- |
| ARA | means Application Reference Architecture. |
| CHADS | means Children Analytics Data Service. |
| CMG | means Child Maintenance Group. |
| CMS | means Child Maintenance Service. |
| CMS 2012 Scheme | means Child Maintenance Service 2012 Scheme. The scheme introduced to support separated parents to work together and set up their own family-based arrangements and support families who are unable to make arrangements themselves. |
| CMS 2012 System | means IT system to administer the 2012 Scheme. |
| DDaT | means Digital, Data and Technology - Capability Framework that describes the job roles in the Digital, Data and Technology Profession. |
| DWP | means The Department for Work and Pensions, The Buyer / Contracting Authority. |
| Incident | an unplanned interruption or a reduction in the quality of an IT service or a failure of a Configuration Item (CI) that has not yet impacted an IT service. Incidents can include failures or degradation of services reported by Users, Technical staff, Service Providers, or automatically from Event monitoring tools |
| Priority 1 | means the priority assigned by the Service Desk when an Incident has a business-critical impact, for example where the Incident results inComplete failure of a Business-Critical Application and/or Business Critical Service affecting all users at one or more Key Sites, or all users at two or more secondary sites; or  1. Delay to, or the inaccurate production of Business-Critical outputs |
| Priority 2 | means the priority assigned by the Service Desk when an Incident has a significant impact, for example where the [2] Incident results inComplete failure of a Business-Critical Application and or Business Critical Service affecting all users at a single secondary site; orPartial failure of a Business-Critical Application and or Business Critical Service affecting all users at one or more Key Sites, or all users at two or more secondary sites; or  * 1. Complete failure of a Secondary Application and/or Secondary Service affecting all users at one or more Key Sites |
| Priority 3 | means the priority assigned by the Service Desk when an Incident results in:Partial failure of a Business-Critical Application and or Business Critical Service affecting all users at a single secondary site; orComplete failure of a Secondary Application and or Secondary Service affecting all users at one or more secondary sites; orPartial failure of a Secondary Application and or Secondary Service affecting all users at one or more Key Sites; orPartial failure of a Secondary Application and or Secondary Service affecting all users at two or more secondary sites; orFailure of a piece of equipment |
| Priority 4 | means the severity assigned by the Service Desk when an Incident resultsPartial failure of a Secondary Application and or Secondary Service affecting all users at one secondary site; orIncident or occurrence which is not a Priority 1, Priority 2 or Priority 3 |
| TCS BaNCS | means Core banking software suite developed by Tata Consultancy Services. |

# scope of requirement

## TCS BaNCS is a transaction-based system which supports accounting and General Ledger reporting.

## The objective of CMG is to ensure that our clients, citizens, and employers, have access to a reliable, available, wholly supported and performant CMS2012 Service. To achieve this, it requires an application development and live service provider that can manage and deliver business requirements that impact TCS BaNCS to ensure a stable CMS2012 and ChADS systems, support DWP in planning, developing, and assuring the portfolio of approved business and technology CMS2012 change.

## DWP wishes to appoint a Supplier who possess the required digital capabilities. The appointed Supplier will provide application development and live service support of TCS BaNCS, which is a core component of the CMS 2012 system.

# The requirement

## Where business and functional changes are made to the CMS 2012 System these may have an impact on the TCS BaNCS component. The Supplier will be required to impact such changes and be required to undertake the necessary application development activity to update TCS BaNCS to ensure CMS 2012 remains operational and manage and resolve incidents that relate to TCS BaNCS.

## The Supplier will deliver outcomes for required regular releases to deploy a range of additional business and technical requirements whilst also supporting the delivery of the wider DWP and Children’s transformation initiatives and provide live support to the production system, within a complex multi-application, multi-supplier environment, to ensure it remains current with legislation and optimised for performance and service.

## The Supplier will undertake the following activities supporting Children and Families delivery teams as detailed below:

## Application Development

* Core CMS 2012 - delivering priority business and functional changes and problem fixes to TCS BaNCS, that result from changes implemented to the Core CMS2012 system, and other CMG applications to achieve operational efficiencies and stable business processing.
* Common Platforms – maintain mature CI/CD pipelines, DevOps support, IBM re hosting to AWS and building prioritised common platform solutions.
* Data – development and support for Children Analytical Data Service (ChADS), ensuring data feeds from TCS BaNCS are updated and maintained.
* Projects – management of prioritised digital projects and discoveries relating to or impacting TCS BaNCS.
* Online – where impacting TCS BaNCS, support the design, development and enhancement of online products such as Options, Online Application and Portal applications.

## Live Service Support

## Common Platforms – support for existing CMS2012 TCS BaNCS environments,

## Live Service Team – in relation to TCS BaNCS support live services for CMS2012, ChADS and DXM, within the Service Management Framework.

## The Supplier will be expected to provide the following deliverables:

## Application Development

Project and Programme Management

* Portfolio Prioritisation, working with DWP to prioritises the backlog.
* Estimating and technical sizing, working with DWP to estimate the cost and time estimates of items in the backlog.
* High- and low-level project planning, building the requisite sprint and delivery plans to deliver the agreed changes.
* Capacity and resource management and monitoring.
* Risk, assumption, constraint and dependency management, documenting and managing all key project risks, assumptions, constraints and dependencies.

**Solution Architecture and Design**

* Producing high level and detailed solution options for decision at governance forums.
* Producing and maintaining Design and Architecture artefacts (e.g. HLTAD, HLDD).
* Working with DWP stakeholders to ensure that all technical solutions produce the best business outcomes.

**Development**

* A capacity driven development team broadly aligned to ensure capability coverage across all platform components. The team will work to develop changes associated with the prioritised CMS2012 backlog requirements. Developing the code for all target environments, developing and running unit tests to assure quality.
* Supporting the resolution of application issues throughout the development and implementation cycle.

**Testing and Test Support**

* Working with DWP stakeholders to develop appropriate test approach documents, test strategy documents and test plans.
* Development of increased test automation capability across the estate.
* Maintenance of supplier-controlled test environments.
* Support of the remediation of CMS2012 test environments.

**Infrastructure Support**

* Provisioning of infrastructure to support CMS2012 change.
* Maintenance and support of all supporting supplier-controlled environments.
* Input into infrastructure migration initiatives.

**Live Service Support**

* Investigate and resolve incidents relating to the BaNCS application and provide technical support in collaboration for incidents pertaining to CMS2012, Online and ChaDS.
* Working with DWP stakeholders for identifying service and capacity improvements which could be implemented within the BaNCS application
* Identifying and analysing problem fixes which need to be implemented for BaNCS.
* Collaborating with other squads, DWP stakeholders and partners for implementing their changes in live for CMS2012, Online and ChADS systems, in alignment with their or BaNCS requirements.

## Standby, Callout and Planned Out of Hours Services

## There is a requirement for the Supplier to be contracted on an out of hour’s basis in certain instances under this Contract. Where such services will be requested the Charges shall be agreed in advance with the Buyer.

## The Supplier shall provide its Services with adequate overlap between shifts to facilitate handover and takeover activities.

## Standby Services: The ‘Standby Services’ means those Services provided by the Supplier whereby particular Service is not being actively provided. Such Services shall only be used in relation to Application Maintenance and Support services. The duration of the Standby Services is detailed below:

| **Standby Services Shift Details** | |
| --- | --- |
|  | **Shift Duration** |
| Working Days | 20:30 to 07:30 |
| Weekends | Friday 20:30 to Monday 07:30 |
| Public Holidays | Whole day (07:30 to 07:30 next day) |

## Call Out Services: The “Call Out Services” means the communication by or on behalf of the Buyer to the Supplier during a period of Stand-by and the Supplier’s obligation to respond to and attend to said incident. The scope of services in relation to Application Maintenance and Support will be limited to following:

1. The Buyer shall call out the Supplier resources for resolving incidents or activities deemed critical for live service stability.
2. The Supplier shall provide appropriate resolution or workaround or set of instructions to restore the services.
3. In the event of call out, the Supplier resource on standby shall engage other resources as required.

* Out of Hours Services: The “Out of Hours Services” means those services provided by the Supplier, which have been agreed in advance by the Buyer and the Supplier, during periods where services are required outside of the relevant Working Hours. Such Services shall be used for both Application Development and Application Maintenance and Support services.
* Priority 1 incident:
* Priority 2 incident:

## DWP Working Hours:

Monday to Friday: 07:30 to 20:30

Saturday: 07:30 to 17:00

Sunday: No Service. (Although Overtime may be worked between 07:30 - 15:00 depending on business needs)

# key milestones and Deliverables

## Deliverables to be provided during the Contract Period this Contact will be determined by the DWP Digital Children product backlog. These will consist of business, functional, and transformational change products that either relate directly to or have an impact on TCS BaNCS.

## This work programme will naturally be subject to change, due re-prioritisation, policy/legislative changes etc., so it is not possible at this point to articulate outcomes at the lowest level.

## Delivery is undertaken using Agile methodology based of a cycle of 8-week sprints.

# MANAGEMENT INFORMATION/reporting

## Supplier shall provide the following management information, where applicable to the Contract:

| Type of Information | Services this requirement applies to | Required regularity of Submission |
| --- | --- | --- |
| Financial Reports | | |
| Detailed breakdown of actual and forecast charges against the contract. | Application development and live service support. | by the 10th of each Month. |
| Performance Metrics | | |
| Performance Monitoring Report. | Detail of the performance by the Supplier against each of the Performance Indicators. | Within ten (10) Working Days of the end of each Service Period. |
| Balanced Scorecard Report. | Summarises the Supplier’s performance against each of the Key Performance Indicators over the relevant Service Period. | Quarterly from the commencement of the Contract. |
| Live Service Support (LSS) Dashboard. | Live Service Support. | Weekly |
| CMT Service Management Report. | Live Service Support | Monthly |
| Key Subcontractors and Supply Chain Governance | | |
| Key Subcontractors Report. | Notified Key Sub-Contractors. | With each replacement / approved appointment or variation. |
| Supply Chain Transparency Information Report. | Visibility of Supply Chain Spend. | Within ten (10) Working Days from end of each Financial Year. |
| Supply Chain Visibility Report. | Visibility of Sub-Contract Opportunities in the Supply Chain. | Quarterly from the commencement of the Contract. |
| Social Value | | |
| Social Value. | Detail of the performance by the Supplier against the social value key performance indicators (SV KPIs). | Quarterly from the commencement of the Contract. |
| Security | | |
| HMG Baseline Personnel Security Standard - Contractor’s Declaration. | Confirmation that all staff and approved sub-contractors have been assessed in accordance with the requirements of the HMG Baseline Personnel Security Standard. | Annually from the commencement of the Contract. |

# volumes

## The current service is delivered from both an on-shore and off-shore location. The table below illustrates the current monthly resource profile providing the service:

| **Service** | **Role** | **FTE** | **Skill Level** |
| --- | --- | --- | --- |
| AD | Software Engineer | 1.00 | Working |
| AD | Software Engineer | 1.00 | Working |
| AD | Business Architect | 1.00 | Working |
| AD | Business Architect | 1.00 | Working |
| AD | Infrastructure Engineer | 1.00 | Practitioner |
| LSS | Service Manager | 1.00 | Awareness |
| LSS | Software Engineer | 1.00 | Expert |
| LSS | Infrastructure Engineer | 1.00 | Working |

# continuous improvement

## The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract Period.

## The Supplier should present new ways of working to the Buyer during quarterly Contract review and supplier relationship management meetings.

## Changes to the way in which the Services are to be delivered must be brought to the Buyer’s attention and agreed prior to any changes being implemented.

# Sustainability

## DWP must at all times be seen to be actively promoting Sustainable Development through its environmental, social and economic responsibilities.

* In delivering the Services, the Supplier shall and shall ensure that its Supplier Personnel assist and cooperate with DWP.
* In delivering the Services, the Supplier shall prepare a Sustainable Development Policy Statement giving, for each organisation involved in delivery of the Contract an overarching commitment to: -

1. dispose of Contract waste in a legal manner (i.e. waste is disposed of via a registered waste collector, the Waste Electrical and Electronic Equipment (WEEE) regulations are adhered to where relevant);
2. reduce energy consumption;
3. promote waste management including recycling;
4. promote green or public transport;
5. promote Corporate Social Responsibility (CSR); and
6. the Sustainable Development Policy and that of continuous improvement which should be signed and dated by senior management.

## In delivering the Services, the Supplier shall prepare and deliver a Sustainable Development Plan which should be used to turn the commitment shown in the Sustainable Development Policy into action and which as a minimum, detail how each organisation involved in delivery of the Contract will:

1. reduce their Environmental footprint;
2. contribute to Social sustainability and;
3. drive Economic sustainability.

# quality

## The Supplier shall comply with the following Standards:

## The technology code of practice - <https://www.gov.uk/guidance/the-technology-code-of-practice>.

* + Open Standards principles - <https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles>.
  + Open standards for government data and technology - <https://www.gov.uk/government/collections/open-standards-for-government-data-and-technology>.
  + The Supplier shall produce full and detailed technical architecture documentation for the Supplier Solution in accordance with Good Industry Practice.
  + **Accessible Digital Standards:** The Supplier shall comply with (or with equivalents to):
    1. the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.1 Conformance Level AA; and
    2. ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability.
  + **Service Management:**
    1. ITIL v4;
    2. ISO/IEC 20000-1 2018 “Information technology — Service management – Part 1”;
    3. ISO/IEC 20000-2 2019 “Information technology — Service management – Part 2”;
    4. ISO 10007: 2017 “Quality management systems – Guidelines for configuration management”; and
    5. ISO 22313:2020 “Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301” and, ISO/IEC 27031:2011 and ISO 22301:2019.
  + **DWP Security Standards:** <https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards>.

# PRICE

## For the purpose of evaluation of the commercial envelope, bidders will be scored based on the overall cost resource profile set out in the Attachment 4 Price Schedule.

## The Buyer has provided an indicative resource profile representing current consumption, detailing the service, DDaT role, skill level and number of FTE.

## Bidders are asked to provide a rate for each role listed and indicate the location, by stating if they intend to undertake this from either from an on-shore or off-shore location.

## The cost will be determined by multiplying the proposed FTE and man-day rate for each role, which will then be multiplied by 232 working days to provide an annual charge for evaluation purposes. All prices shall be in GBP and exclusive of VAT.

## In addition, the Bidder is also asked to provide the proposed charging mechanism for the Standby, Call-Out and Out of Hours services to support their proposal.

## The Buyer will use one or more of the below Charging methods to be specified in the Order Form:

* + Capped Time and Materials (CTM).
  + Time and Materials (T&M).
  + Fixed Price.
* A combination of two or more of the above Charging methods

## The rate card shall be incorporated into the Contract and the Supplier shall charge the Buyer a rate no greater than those set out in the rate card for the Supplier Personnel undertaking that element of work on the Deliverables.

## Any expenses charged for each Working Day for each Supplier Personnel, must be in accordance with the Buyer’s expenses policy attached below (which may change from time to time) and agreed in advance with the Buyer’s Commercial Lead.

## 

# STAFF AND CUSTOMER SERVICE

## The Supplier shall provide a sufficient level of resource throughout the Contract Period in order to consistently deliver a quality service.

## The Supplier Personnel assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard, including:

### Technical skills in application development and support of TCS BαNCS product, Microfocus Server Express and TCS BαNCS Adapter, and other CMS2012 technologies such as Siebel and BPM.

### Experience of operating BaNCS in a comparable integrated environment.

### Experience of delivering a combined live support and development capability using a wide range of methodologies including agile and waterfall.

### Experience of delivering major change via concurrent releases and live support services.

## The Supplier shall ensure that staff understand the Buyer’s vision and objectives and will provide excellent customer service to the Buyer throughout the Contract Period.

# service levels and performance

## The Buyer will measure the quality of the Supplier’s delivery against the Digital Service Management KPIs set out in the attached document below:

## 

## The diagram below illustrates the anticipated governance model to be used for this Contract. Each board and meeting have an agreed term of reference that sets out its purposes and objectives.

## Performance will be managed through close engagement with experienced DWP Digital leads. Outcomes delivered will be assured against the agreed quality criteria for each requirement with performance managed through regular meetings to discuss and review performance including; monthly engagement meetings with supplier leadership teams; sprint planning meetings; sprint review meetings; sprint retrospectives.

## In addition to Service Levels detailed above, the Buyer will be using balanced scorecard to monitor performance and the health of the supplier relationship, see the embedded document below.

## 

# Security and CONFIDENTIALITY requirements

## The Supplier will comply with the DWP Security Policy and Standards which can be accessed online at: <https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards>.

## All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard, which can be found online at: <https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>.

## The Buyer and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Buyer to determine which roles require additional vetting and a specific national security vetting clearance (e.g., a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which process Buyer Data or data which, if it were Buyer Data, would be classified as OFFICIAL-SENSITIVE.

## The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 16.2 and 16.3 to be involved in the management and/or provision of the Services except where the Buyer has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.

## The Supplier shall ensure that the HMG Baseline Personnel Security Standard - Contractor’s Declaration is completed within four (4) weeks of the Commencement Date and submitted for each calendar year thereafter within one month of the end of each calendar year.

# payment AND INVOICING

## Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

## For products and deliverables that have been agreed by the Parties to be charged on a Time and Material basis, the Supplier shall submit, as soon as possible and in any case within ten (10) Working Days, an invoice and Supporting Documentation in a format specified by the Buyer for the Charges incurred during that Payment Period to the Buyer principal contact and/or other nominated representative to verify the accuracy of any invoice submitted. For the purposes of this paragraph the Payment Period is defined as one calendar month.

## For products and deliverables that have been agreed by the Parties to be charged on a Fixed Price basis the Supplier shall, on the Achievement of a Milestone, be entitled to invoice the Buyer for the Milestone Payment associated with that Milestone.

## Service Charges shall be invoiced by the Supplier for each Service Period in arrears. The Service Period is defined as one calendar month.

## Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

## Invoices should be submitted to:

**REDACTED TEXT under FOIA Section 40, Personal Information**

## The Buyer shall make payment to the Supplier within thirty (30) days of verifying that the invoice is valid and undisputed.

## Unless the Parties agree otherwise in writing, all Supplier invoices shall be paid in sterling by electronic transfer of funds to the bank account that the Supplier has specified on its invoice.

# CONTRACT MANAGEMENT

## In consideration of the strategic and critical nature of the services a commercial lead will be appointed to oversee regular contract management arrangements that cover the day-to-day management of the Contract such as performance, minor changes and the escalation procedure for difficulties. As part of this a contract management plan will be produced detailing all the key aspects of the Contract and contractual obligations will be managed via on obligations tracker, which will be used to inform the assessment for the relevant balanced scorecard KPI.

## All contract management activities will be carried out in accordance the relevant Commercial Agreement and the Contract terms and conditions.

## Formal disputes will be managed in accordance with the framework Terms. Every effort will be made to resolve any issues at the earliest opportunity and at the lowest level through the governance structure before they turn into escalations as disputes. Maintaining a healthy relationship with the Supplier is a key part of the SRM regime that will be followed for this Contract.

## The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of the Contract can be fully realised.

## Contract Review meeting will be held as per the governance structure.

## Attendance at Contract Review meetings shall be at the Supplier’s own expense.

# Location

## Current arrangements are that resources will work from a remote location, until guidelines change.

## Under normal circumstances the main DWP location for the Services will be carried out at the DWP Newcastle Hub:

**REDACTED TEXT under FOIA Section 40, Personal Information**

## A hybrid working practice may be adopted in the future with resources and Supplier Personnel spending 40% of time in DWP offices and 60% off-site, this will be communicated to the Supplier and specific details will be agreed by the Parties at contract award.

## Suppliers have the opportunity, subject to DWP’s written security approval, to deliver the Services from an off-shore location.

**Attachment 2 – Charges and Invoicing**

**Part A – Milestone Payments and Delay Payments – Not Applicable.**

**Part B – Service Charges – Not Applicable**

**Part C – Supplier Personnel Rate Card for Calculation of Time and Materials Charges**

**REDACTED TEXT under FOIA Section 43 Commercial Interests.**

**REDACTED TEXT under FOIA Section 43 Commercial Interests.**

**Part D – Risk Register - Not Applicable**

| **Column 1** | **Column 2** | **Column 3** | **Column 4** | **Column 5** | **Column 6** | **Column 7** | **Column 8** | **Column 9** | **Column 10** | **Column 12** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk Number** | **Risk Name** | **Description of risk** | **Timing** | **Likelihood** | **Impact (£)** | **Impact (description)** | **Mitigation (description)** | **Cost of mitigation** | **Post-mitigation impact (£)** | **Owner** |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

**Part E – Early Termination Fee (s): N/A** .

**Attachment 3 – Outline Implementation Plan – Supplier to populate**

| **#** | **Milestone** | **Deliverables**  **(*bulleted list showing all Deliverables (and associated tasks) required for each Milestone*)** | **Duration**  **(*Working***  ***Days*)** | **Milestone**  **Date** |
| --- | --- | --- | --- | --- |
| M1 | [Concept Design] | [Statement of Requirements  System/Application Specifications  Interface Specifications  Systems Testing Strategy  Implementation Strategy and Plan  Risk and Issues Management Plan  Outline Disaster Recovery Plan  Project Schedule  Service Management Plan] | **TBC** | **TBC** |
| M2 | [Full Development] | [Design Verification Reports  Design Validation Reports  Change Management Plan  System/Application Implementation Plan  Risk and Issues Management  Project Schedule  Service Management Plan] | **TBC** | **TBC** |
| M3 | [System User Testing] | [System Test Report  Risk and Issues Management Plan  Project Schedule  Service Management Plan  Defects Log  Final Inspection and Testing Report] | **TBC** | **TBC** |
| M4 | [User Readiness for Service] | [Training Plan  Risk and Issues Log  Implementation Plan  Operations Plan  Data Conversion & Cutover Plan  Project Schedule  Service Management Plan] | **TBC** | **TBC** |
| M5 | [Implementation] | [Implementation Plan  Training Scripts] | **TBC** | **TBC** |
| M6 | [In Service Support] | [Post Implementation Report  Data Conversion and Cut-Over Plan  Service Delivery Reports  Risk and Issues Log  Service Management Plan  Defects Log] | **TBC** | **TBC** |

**Attachment 4 – Service Levels and Service Credits**

**Service Levels and Service Credits**

**Please refer to Attachment 1 – Services Specification, of this document. The details are as set out within Section 15. Service Levels and Performance.**

**Service Credit Calculation**

**Please refer to Attachment 1 – Services Specification, of this document. The details are as set out within Section 15. Service Levels and Performance.**

**Attachment 5 – Key Supplier Personnel and Key Sub-Contractors**

### The Parties agree that they will update this Attachment 5 periodically to record any changes to Key Supplier Personnel and/or any Key Sub-Contractors appointed by the Supplier after the Commencement Date for the purposes of the delivery of the Services.

**Part A – Key Supplier Personnel – Supplier to populate**

[Guidance Note: Insert details of Key Supplier Personnel, their Key Role(s) and Duration in the below table or delete the table in its entirety and insert Not Applicable if there is no Key Supplier Personnel]

| Key Supplier Personnel | Key Role(s) | Duration |
| --- | --- | --- |
| **REDACTED TEXT under FOIA Section 43 Commercial Interests.** |  | [Contract Period or insert alternative timescale] |
| **REDACTED TEXT under FOIA Section 43 Commercial Interests.** |  | [Contract Period or insert alternative timescale] |
| **REDACTED TEXT under FOIA Section 43 Commercial Interests.** |  | [Contract Period or insert alternative timescale] |

**Part B – Key Sub-Contractors – N/A**

**Attachment 6 – Software – N/A**

### The Software below is licensed to the Buyer in accordance with Clauses 20 (*Intellectual Property Rights*) and 21 (*Licences Granted by the Supplier*).

### The Parties agree that they will update this Attachment 6 periodically to record any Supplier Software or Third-Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

**Part A – Supplier Software**

The Supplier Software includes the following items:

| **Software** | **Supplier (if an Affiliate of the Supplier)** | **Purpose** | **Number of Licences** | **Restrictions** | **Number of Copies** | **Type (COTS or Non-COTS)** | **Term/**  **Expiry** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Part B – Third Party Software – N/A**

The Third-Party Software shall include the following items:

| **Third Party Software** | **Supplier** | **Purpose** | **Number of Licences** | **Restrictions** | **Number of Copies** | **Type (COTS or Non-COTS)** | **Term/**  **Expiry** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Attachment 7 – Financial Distress – N/A**

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the following shall apply:

**PART A – CREDIT RATING THRESHOLD**

| **Entity** | **Credit Rating (long term)**  *(insert credit rating issued for the entity at the Commencement Date)* | **Credit Rating Threshold**  *(insert the actual rating (e.g. AA-) or the Credit Rating Level (e.g. Credit Rating Level 3)* |
| --- | --- | --- |
| ***Supplier*** | Standard and Poor’s | Standard and Poor’s – Credit Rating Level 10 |
| ***[Guarantor]*** | [etc.] | [etc.] |
| ***[Key Sub-contractor 1]*** | [etc.] | [etc.] |
| ***[Key Sub-contractor 2]*** | [etc.] | [etc.] |

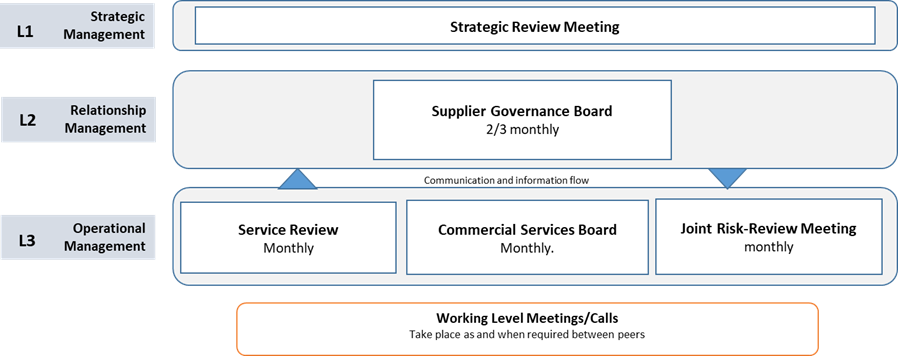
**PART B – RATING AGENCIES**

* Rating Agency 1 - Standard and Poor’s
  + Credit Rating Level 1 = [AAA]
  + Credit Rating Level 2 = [AA+]
  + Credit Rating Level 3 = [AA]
  + Credit Rating Level 4 = [AA-]
  + Credit Rating Level 5 = [A+]
  + Credit Rating Level 6 = [A]
  + Credit Rating Level 7 = [A-]
  + Credit Rating Level 8 = [BBB+]
  + Credit Rating Level 9 = [BBB]
  + Credit Rating Level 10 = [BBB-]

**Attachment 8 – Governance**

**PART A – SHORT FORM GOVERNANCE**

Governance under contract will operate in accordance with the following diagram:



**Attachment 9 – Schedule of Processing, Personal Data and Data Subjects**

This Attachment 9 shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Buyer at its absolute discretion.

* + - 1. The contact details of the Buyer’s Data Protection Officer are: data.protection@dwp.gov.uk
      2. The contact details of the Supplier’s Data Protection Officer are: [Insert Contact details]
      3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
      4. Any such further instructions shall be incorporated into this Attachment 9.

| **Description** | **Details** |
| --- | --- |
| Identity of Controller for each Category of Personal Data | **The Authority is Controller and the Supplier is Processor**  The Parties acknowledge that in accordance with Clause 34.2 to 34.15 of the Call-Off Terms and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:  The Personal Data processed by the Supplier is as set out in the below tab titled “Type of Personal Data”.  In providing application development and live support outcomes, the Supplier does not have access to the live environment and therefore does not have any direct access to Personal Data relating to the Buyer’s customers. However, in instances where the Supplier requires information to resolve incidents or problems, this information is made available to the Supplier by the Buyer and may contain Personal Data (e.g. logs, screenshots).  In addition to having access to Personal Data required to resolve incidents, the Supplier retains contact details for the Buyer’s employees and other suppliers. These are periodically updated as individuals change roles. |
| Duration of the processing | Where the Supplier requests additional information relating to an incident, this information is made available by the Buyer via the Buyer’s TechNow tooling and may include Personal Data. If required, the Supplier may download the information (including any Personal Data) from TechNow to the Buyer provisioned development and tests environments. Once the incident is resolved or the incident is re-directed to another supplier and the incident is not expected to return to the Supplier for further action, the Supplier erases the information (including any Personal Data) from the Buyer provisioned development and test environments subject to appropriate approvals and system access rights.  Personal Data relating to the Buyer’s employees and other suppliers are retained for as long as required. |
| Nature and purposes of the processing | Incidents are raised by the Buyer’s staff/suppliers and may concern individual (or multiple) live customer cases.  In order to resolve incidents relating to deployed Applications, the Supplier may request relevant information to assist them in resolving the incident.  Such information (which may include Personal Data relating to the Buyer’s customers) is made available to the Supplier by the Buyer via TechNow. If required, the Supplier may download this information (including any Personal Data) to the Supplier’s development environment (e.g., to create an anonymised record to support testing of a fix) although such downloads can only be done by onshore Supplier resources.  Where analysis of an incident identifies that amendments are required to customer records, the Supplier may, if requested, provide a scan to identify the affected records but will not have access to those records or the ability to amend those records.  Once the incident is resolved or the incident is re-directed to another supplier and the incident is not expected to return to the Supplier for further action, the Supplier shall erase the information (including any Personal Data) from the Buyer provisioned development and Tests environments subject to appropriate approvals and system access rights.  Regarding contact details for the Buyer’s employees and other suppliers, the Supplier may collect, store and use this Personal Data in order to maintain a directory of valid business contacts to assist effective communication as part of business-as-usual operations. |
| Type of Personal Data | For incident resolution:  Personal Data relating to the Buyer’s customers may include but is not limited to customer name, NINO, date of birth, home address, telephone details, email address, details of benefit claims, pensions, customer health related information, payment details, bank account details etc.  Personal Data relating to the Buyer’s employees and supplier contacts may include but is not limited to name, job title, telephone details, email address etc.  Personal Data related to Supplier employees and supplier may include but is not limited to Supplier Personnel’ profiles, personal information supplied to the Buyer for on-boarding of Supplier resources, etc. |
| Categories of Data Subject | The Buyer’s customers  The Buyer’s employees  Other Buyer suppliers  Supplier Personnel |
| Plan for return and destruction of the data once the processing is complete  UNLESS requirement under union or member state law to preserve that type of data | The Supplier retains information (including Personal Data relating to the Buyer’s customers) on its development environment for no longer than required to resolve the incident to which the information relates. When no longer required, it is deleted.  Personal Data relating to the Buyer’s employees, Supplier, Supplier Personnel and other suppliers and their personnel will be securely disposed of on completion of the Contract Period, including any agreed Extension Period(s). |

**Attachment 10 – Transparency Reports**

| **Title** | **Content** | **Format** | | **Frequency** | |
| --- | --- | --- | --- | --- | --- |
| **Performance Metrics** | | | | |
| Performance Monitoring Report | Detail of the performance by the Supplier against each of the Performance Indicators | | Call-Off Terms Schedule 3 Service Levels, Service Credits and Performance Monitoring Part B – 1.2 | Within ten (10) Working Days of the end of each Service Period |
| Balanced Scorecard Report | Summarises the Supplier’s performance against each of the Key Performance Indicators over the relevant Service Period | | as per Balanced Scorecard template | Quarterly |
| **Performance and Underperformance Management** | | | | |
| Performance Monitoring Report | Detail of the performance by the Supplier against each of the Performance Indicators | | Call-Off Terms Schedule 3 Service Levels, Service Credits and Performance Monitoring Part B – 1.2 | Within ten (10) Working Days of the end of each Service Period |
| **Call-Off Contract Charges** | | | | |
| Contract Financial Report | Breakdown of Suppliers costs, operating expenditure, overheads, profit. | | As appropriate and agreed by the Buyer | Annually from the anniversary of the Effective Date |
| Contract Charges Report | Detailed breakdown of charges against each Statement of Work | | As appropriate and agreed by the Buyer | Monthly |
| **Key Subcontractors and Supply Chain Governance** | | | | |
| Key Subcontractors Report | Notified Key Sub-Contractors | | Order Form - Attachment 5 – Key Supplier Personnel and Key Sub-Contractors – Part B | With each replacement / approved appointment or variation |
| Supply Chain Transparency Information Report | Visibility of Supply Chain Spend | | [Supply Chain Information Report template](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/921463/18.04.10_SME_measures_PPN_118_Annex_C_-_Departmental_Contract_SME_Data_CollectionTemplate_.ods) | Within ten (10) Working Days from end of each Financial Year |
| Supply Chain Visibility Report | Visibility of Sub-Contract Opportunities in the Supply Chain | | As appropriate and agreed by the Buyer | Quarterly |
| **Technical** | | | | |
| Technical Infrastructure and Operating Procedures | Configuration database detailing the technical infrastructure and operating procedures | | As appropriate and agreed by the Buyer | Any variation |
| **Resource Plans** | | | | |
| Key Supplier Staff | Key Supplier Staff | | Order Form - Attachment 5 – Key Supplier Personnel and Key Sub-Contractors – Part A | On replacement of Key Supplier Staff |
| **Social Value** | | | | |
| Social Value | Detail of the performance by the Supplier against the social value key performance indicators (SV KPIs) | | As appropriate and agreed by the Buyer | Quarterly |

**Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses**

**Call- Off Terms**

****

**Additional/Alternative Schedules & Clauses relating to Lot 3d**

****

**Attachment 11 – DWP Security Provisions**

DWP has legal and regulatory obligations to verify that the Suppliers we work with have a reasonable standard of security in place to protect Buyer Data and Buyer assets. DWP is committed to the protection of its information, assets and personnel and expects the same level of commitment from its suppliers (and sub-contractors if applicable). In order to protect the Department appropriately, DWP have recently reviewed its Security Supplier Assurance process and requirements and have made the applicable changes in line with industry good practice.

These changes include but are not limited to:

* Updated ‘Security Schedule’.
* Replacement of ‘Security Management Plans’ with the completion of the ‘Information Security Questionnaire’ as part of the tender submission.
* Compliance with the DWP’s relevant policies and standards, found at [*gov.uk*](https://www.gov.uk/government/publications/data-protection-and-security-of-information-supplying-to-dwp).
* Certification to industry good practice such as ‘ISO27001’/OSO27002 and ‘Cyber Essentials Plus’.

Full information about DWP’s security safeguards and requirements are set out below.

The following DWP Security Provisions shall apply to this Contract during the Contract Period:

1. **Protection of Information:**

Insert after Paragraph 25.5.3(c) of the Framework Agreement a Paragraph 25.5.3 (d) to read as follows:

“(i). The Supplier and any of its Subcontractors, shall not access, process, host or transfer Buyer Data outside the United Kingdom without the prior written consent of the Buyer, and where the Buyer gives consent, the Supplier shall comply with any reasonable instructions notified to it by the Buyer in relation to the Buyer Data in question. The provisions set out in this paragraph shall also apply to Landed Resources.

(ii). Where the Buyer has given its prior written consent to the Supplier to access, process, host or transfer Buyer Data outside the United Kingdom (in accordance with clause (i) above: -

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

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

Definitions:

1. “Buyer 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 Buyer; or

(ii) which the Supplier is required to generate, process, store or transmit pursuant to this Call Off Contract.

1. “Landed Resources” means when the Supplier or its Subcontractor causes foreign nationals to be brought to the United Kingdom to provide the Services.
2. “Law” means any applicable law, Act of Parliament, subordinate legislation including legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, exercise of the royal prerogative, enforceable European Union right including enforceable rights within the meaning of Section 2 of the European Communities Act 1972, regulatory policy, guidance or industry code, judgment of a relevant court of law, regulation, directive, order, mandatory guidance, code of practice and/or requirements or any Regulatory Body of which the Supplier is bound to comply.
3. “Regulatory Bodies” means those government departments and regulatory, statutory and other entities, committees, ombudsmen and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in the Call Off Contract or any other affairs of the Buyer and “Regulatory Body” shall be construed accordingly.”
4. **Security Requirements:**

2.1. Subject to paragraph 2.2 below, Part B Long Form Security Requirements of Schedule S3 (Security Requirements) shall apply to this Contract.

2.2. Paragraph 3.4.2 Part B Long Form Security Requirements of Schedules S3 shall be replaced with:

“ISO27001 Compliance, Certification and Audit:

“The Supplier shall, and shall procure that any subcontractor (as applicable) shall, meet the relevant standards and obtain and maintain certification to ISO/IEC 27001 and ISO/IEC27002 (the “**ISO Certificate**”) in relation to the Services during the Contract Period. The ISO Certificate shall be provided by the Supplier to the Buyer on the dates as agreed by the Parties.

If the Supplier and subcontractor are not ISO27001 and ISO27002 certified, the Buyer can agree a plan and timescale for certification, and the Buyer reserves the right to amend and update the Order Form to reflect the Supplier and subcontractors’ certification”.

1. **Cyber Essentials Plus Scheme:**

3.1. Part B Long Form Security Requirements of Schedule S3 (Security Requirements) shall be amended in accordance with paragraph 3.2 below.

3.2. After Paragraph 9 of Part B Long Form Security Requirements of Schedule S3 (Security Requirements), insert paragraph 10 titled “Cyber Essentials Plus” as set out in paragraph 3.3 below.

3.3. Paragraph 10 of Part B Long Form Security Requirements of Schedule S3 (Security Requirements) shall read as follows:

“10. **CYBER ESSENTIALS PLUS SCHEME**

10.1. In addition to the Supplier’s obligation under Paragraph 9 of the Framework Agreement, the Supplier shall, and shall procure that any sub-contractor (as applicable) shall, obtain and maintain certification to Cyber Essentials Plus (the “**Cyber Essentials Plus Certificate**”) in relation to the Services during the Contract Period. The Cyber Essentials Plus Certificate shall be provided by the Supplier to the Buyer annually on the dates as agreed by the Parties.

10.2. The Supplier shall notify the Buyer of any failure to obtain, or the revocation of, a Cyber Essentials Plus Certificate within 2 Working Days of confirmation of such failure or revocation. The Supplier shall, at its own expense, undertake those actions required in order to obtain a Cyber Essentials Plus Certificate following such failure or revocation. For the avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Plus Certificate during the Contract Period after the first date on which the Supplier was required to provide a Cyber Essentials Plus Certificate in accordance with paragraph 10.1 (regardless of whether such failure is capable of remedy) shall constitute a material Default entitling the Buyer to exercise any of its rights under clause 35 of the Call-Off Terms.

Definitions:

1. “Cyber Essentials Plus”: shall mean the Government-backed, industry-supported scheme managed by the NCSC with higher level of security requirements to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
2. “NCSC”: shall mean the National Cyber Security Centre or its successor entity (where applicable).
3. **Risk Management:**

4.1. Part B Long Form Security Requirements of Schedule S3 (Security Requirements) shall be amended in accordance with paragraph 4.2 below.

4.2. After paragraph 10 of Part B Long Form Security Requirements of Schedule S3 (Security Requirements), insert paragraph 11 titled “Risk Management” as set out in paragraph 4.3 below.

4.3. Paragraph 11 of Part B Long Form Security Requirements of Schedule S3 (Security Requirements) shall read as follows:

“11.1. 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 Buyer’s Security Requirements are met (the **Risk Assessment**). The Supplier shall provide the Risk Management Policy to the Buyer upon request within 10 Working Days of such request. The Buyer may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Buyer’s Security Requirements. The Supplier shall, at its own expense, undertake those actions required in order to implement the changes required by the Buyer within one calendar month of such request or on a date as agreed by the Parties.

11.2. 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 Buyer. The Supplier shall provide the report of the Risk Assessment to the Buyer, 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 Buyer 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.

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

11.4. The Supplier shall and shall procure that any subcontractor (as applicable) shall, co-operate with the Buyer in relation to the Buyer’s own risk management processes regarding the Services provided for under this Call Off Contract and Framework Agreement.

11.5. 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 provision. Any failure by the Supplier to comply with any requirement of this paragraph (regardless of whether such failure is capable of remedy), shall constitute a Material Default entitling the Buyer to exercise any of its rights under clause 35 of the Call-Off Terms.

Definition:

1. “Buyer’s Security Requirements”: means the Buyer’s security requirement set out in the Call Off Contract which include the requirements set out in Part B Long Form Security Requirements of Schedule S3 (Security Requirements) and this Attachment 11 of this Order Form.
2. “Contractor’s Systems Environment”: means any ICT systems provided by the Supplier (and any sub-contractor) which are or may be used for the provision of the Services.
3. “Risk Profile”: shall mean a description of any set of risks. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable”.
4. **Security Audit and Assurance – Information Security Questionnaire (ISQ)**

5.1. Part B Long Form Security Requirements of Schedule S3 (Security Requirements) shall be amended in accordance with paragraph 5.2 below.

5.2. After paragraph 11 of Part B Long Form Security Requirements of Schedule S3 (Security Requirements), insert paragraph 12 titled “Security Audit and Assurance” as set out in paragraph 5.3 below.

5.3. Paragraph 12 of Part B Long Form Security Requirements of Schedule S3 (Security Requirements) shall read as follows:

12.1. “The Supplier shall, and shall procure that any subcontractor (as applicable) shall, complete the information security questionnaire in the format stipulated by the Buyer (the “**Information Security Questionnaire**  to be provided to the Supplier by the Buyer”) at least annually or at the request by the Buyer. The Supplier shall provide the completed Information Security Questionnaire to the Buyer within one calendar month from the date of request.

12.2. The Supplier shall conduct Security Tests to assess the Information Security of the Supplier’s Systems Environment and, if requested, the Buyer’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 Tiger scheme and, ii) in respect of any Security Test to which PCI DSS (The Payment Card Industry Data Security Standard) 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 Buyer’s System Environment or (iii) at the request of the Buyer 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 Buyer. 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 Buyer in its absolute discretion.

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

12.4. Where the Supplier provides code development services to the Buyer, the Supplier shall comply with the Buyer’s Security Requirements in respect of code development within the Supplier’s Systems Environment and the Buyer’s Systems Environment.

12.5. Where the Supplier provides software development services, the Supplier shall comply with the code development practices specified in Framework Schedule 2, in the Buyer’s Security Requirements and Services Specification as set out in Attachment 1 to the Order Form above.

12.6. The Buyer, 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 Buyer’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 Buyer at its absolute discretion. The Supplier shall provide all such co-operation and assistance in relation to any Security Test conducted by the Buyer as the Buyer may reasonably require.

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

12.8. The Supplier shall, and shall procure that any subcontractor (as applicable) shall, maintain at least annual renewals of **SOC1T2** and **SOC2T2** in accordance with **SSAE 16** and/or **ISAE 3402** during the Contract Period and provide the Buyer with a copy of the applicable **SOC1T2** report and **SOC2T2** report on the dates as agreed by the Parties.

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

12.10. In addition to the provisions set out in paragraphs 11.1 to 11.10, the Supplier shall provide a bridge letter in relation to SOC1T2 and SOC2T2 at the reasonable request of the Buyer. The Supplier shall seek approval of the Buyer as to the content and format of such bridge letter in advance and shall be provided within one calendar month of the Buyer’s request.

12.11. The Buyer shall schedule regular security governance review meetings which the Supplier shall, and shall procure that any subcontractor (as applicable) shall, attend.

Definitions:

1. “Buyer Assets” mean any Buyer Devices and Buyer Data.
2. “Buyer 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 Buyer; or

(ii) which the Supplier is required to generate, process, store or transmit pursuant to this Call Off Contract.

1. “Buyer Devices”means any asset that provides an ICT function and is used by the Buyer to conduct its business and operations.
2. “Buyer’s Systems Environment” means all of the Buyer’s ICT systems which are or may be used for the provision of the Services.
3. “CHECK” shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.
4. “CREST” shall mean the internally recognised scheme for authorised penetration test.
5. “NCSC” shall mean the National Cyber Security Centre or its successor entity (where applicable).
6. “Party” or “Parties”shall be construed accordingly to mean a party to this Call-Off Contract of this Framework Agreement.
7. “Penetration Test” shall mean a simulated attack on any Buyer’s Assets, the Buyer’s Systems Environment (or any part thereof) or the Supplier’s Systems Environment (or any part thereof).
8. “ICT” means information and communications technology.
9. “Information Security” shall mean: the protection and preservation of:
   1. the confidentiality, integrity and availability of any Buyer’s Assets, the Buyer’s Systems Environment (or any part thereof) and the Supplier’s Systems Environment (or any part thereof);
   2. related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and
   3. compliance with all Law applicable to the processing, transmission, storage and disposal of Buyer Assets.
10. “Security test” shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.
11. “Supplier’s Systems Environment” means any ICT systems provided by the Supplier (and any subcontractor) which are or may be used for the provision of the Services.
12. “Tiger scheme”shall mean a scheme for authorised penetration tests which scheme is managed by USW Commercial Services Ltd”.
13. **Security Policies and Standards:**

7.1. Part B Long Form Security Requirements of Schedule S3 (Security Requirements) shall be amended in accordance with paragraph 7.2 below.

7.2. After paragraph 3.5.13 of Part B Long Form Security Requirements of Schedule S3 (Security Requirements), insert paragraph 3.5.14 titled “Security Policies and Standards” as set out in paragraph 7.3 below.

7.3. The following paragraphs are inserted after paragraph 3.5.13 of Part B Long Form Security Requirements of Schedule S3 (Security Requirements) as follows:

3.5.14. “The Supplier shall, and shall procure that any subcontractor (as applicable) shall, comply with the Security Policies and Standards set out in Annex A and B below (further names and link to the Annex A set out below).

3.5.15. Notwithstanding the foregoing, the Buyer’s Security Requirements applicable to the Services provided under this Framework 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 Buyer’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 Buyer’s Security Requirements resulting from such Operational Change (if any) shall be agreed by the Parties and documented in the relevant Operational Change Confirmation.

3.5.16. The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Buyer’s Security Policies and Standards”.

**ANNEX A: BUYER 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:

1. Acceptable Use Policy
2. Information Security Policy
3. Physical Security Policy
4. Information Management Policy
5. Email Policy
6. Technical Vulnerability Management Policy
7. Remote Working Policy
8. Social Media Policy
9. Forensic Readiness Policy
10. SMS Text Policy
11. Privileged Users Security Policy
12. User Access Control Policy
13. Security Classification Policy
14. Cryptographic Key Management Policy
15. HMG Personnel Security Controls – May 2018

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

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

**ANNEX B: BUYER SECURITY STANDARDS**

The Security Standards are published on:

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

1. SS-001 - Part 1 - Access & Authentication Controls
2. SS-001 - Part 2 - Privileged User Access Controls
3. SS-002 - PKI & Key Management
4. SS-003 - Software Development
5. SS-005 - Database Management System Security Standard
6. SS-006 - Security Boundaries
7. SS-007 - Use of Cryptography
8. SS-008 - Server Operating System
9. SS-009 - Hypervisor
10. SS-010 - Desktop Operating System
11. SS-011 - Containerisation
12. SS-012 - Protective Monitoring Standard for External Use
13. SS-013 - Firewall Security
14. SS-014 - Security Incident Management
15. SS-015 - Malware Protection
16. SS-016 - Remote Access
17. SS-017 - Mobile Devices
18. SS-018 - Network Security Design
19. SS-019 - Wireless Network
20. SS-022 - Voice & Video Communications
21. SS-023 - Cloud Computing
22. SS-025 - Virtualisation
23. SS-027 - Application Security Testing
24. SS-028 - Microservices Architecture
25. SS-029 - Securely Serving Web Content
26. SS-030 - Oracle Database
27. SS-031 - Domain Management
28. SS-033 - Patching
29. **Cyber Security Information Sharing Partnership:**

8.1. Part B Long Form Security Requirements of Schedule S3 (Security Requirements) shall be amended in accordance with paragraph 8.2 below.

8.2. After paragraph 13 of Part B Long Form Security Requirements of Schedule S3 (Security Requirements), insert paragraph 14 titled “Cyber Security Information Sharing Partnership” as set out in paragraph 8.3 below.

8.3. Paragraph 14 of Part B Long Form Security Requirements of Schedule S3 (Security Requirements) shall read as follows:

14.1. The Supplier shall be a member of the Cyber Security Information Sharing Partnership during the Call Off Contract and for the duration of the Contract Period. The Supplier shall participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.

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

Definitions.

A. “NCSC”: shall mean the National Cyber Security Centre or its successor entity (where applicable).

B. “Supplier Risk Management Policy”: shall mean Supplier’s policies and processes for risk management 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 Buyer’s Security Requirements are met.