**Call-Off Schedule 1 (Transparency Reports)**

1.1 The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1

[(https://www.gov.uk/government/publications/procurement-policy-note-0117update-to-transparency-principles)](https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.

1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.

1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.

1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

**Annex A: List of Transparency Reports**

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | **Content** | **Format** | **Frequency** |
| AMS Service – Performance Review | KPIs against agreed SLA | F2F, Remote and Report | Monthly |
| AMS Service – Spend Review | Spend Analysis against Utilisation against functional area | F2F, Remote and Report | Monthly |
| Smart Automated Regression Testing | Automated Testing Volumes by Module | F2F, Remote and Report | Monthly |
| Smart Test – Gold Service | Issue Tracking | Email, Online Tracker contained within Smart Tenant and Remote/Online Session | Weekly |
| Quarterly Business Review (AMS and Smart Services) | Business Review of all activities contained with contract and forecasting to ensure delivery of service | F2F/Onsite (or Remote) and Supporting Reporting Info | Quarterly |
| Strategic Business Review | Annual Performance Contract/Relationship Appraisal  Overall review of Service scope  Innovation/Continuous Improvement Proposals  High Level Business Update | F2F/Onsite (or Remote) and Supporting Reporting Info | Yearly |

**Call-Off Schedule 5 (Pricing Details)**

**APPLICATION MANAGEMENT SERVICES (“AMS”)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Charges** | **Year 1** | **Year 2\*** | **Year 3\*** | **Year 4\*** | **Year 5\*** |
| Number of Pre-Paid Hours (AMS) Committed | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| Pre-Paid Hourly Rate (AMS) | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| Total Estimated Annual Charge | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |

\*AMS Hourly Rates will increase in line with annual RPI from 1st May 2023.

**Pre-Paid Hours**

* AMS invoices will be raised quarterly in advance.
* AMS is provided on a time and materials basis and subject to available Pre-Paid Hours.
* All Pre-Paid Hours must be used within the Service Period or they will lapse.
* No refund or credit will be given at the end of the Service Period for unused Pre-Paid Hours.
* Where the Customer renews AMS for a further period of twelve (12) months (or more) then provided that there is no contractual break in the Service Period, 20% of any unused Pre-Paid Hours remaining at the end of the expiring Service Period may be carried over into a renewal Order Form.
* Any hours carried over into a renewal will expire after 3 months.
* Additional Pre-Paid Hours may be purchased at any time during the Service Period using a Change Request Form.

The breakdown of the number of Pre-Paid Service Management Hours and Pre-Paid Hours (AMS) per year above are estimates only. Customer will be invoiced for actual time spent in the provision of AMS and/or Service Management at the relevant Pre-Paid Hourly Rate.

**Project Work**

The Pre-Paid Hourly Rate is for AMS.

* Customer can request that Kainos carries out Project Work under this Order Form.
* Where any individual Project exceeds forty (40) hours, then the current rate card (not the Pre-Paid hourly rate) will be apply.
* To fund agreed Project Work, the Customer may either:
  + use its available Pre-Paid Hours (where the Project Work is less than forty (40) hours); OR
  + use its available Pre-Paid Hours (where the Project Work is more than forty (40) hours) paying the difference between the Pre-Paid Hourly Rate and the rate card hourly rate; OR
  + purchase additional hours for the Project Work at the rate card.

|  |  |
| --- | --- |
| **Additional Rates** |  |
| On-Call Hourly Rate for each hour of AMS coverage outside of Service Hours | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| On-Call Hourly Call Out Charging Rate | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| Customer Requested Overtime Rates | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |

Project Rate Card

|  |  |
| --- | --- |
| **Role** | **Rate** |
| Client Director | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| Engagement Manager | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| Test / Change Manager | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| Lead Consultant | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| Consultant | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |

**SMART SUBSCRIPTION SERVICES**

|  |  |  |
| --- | --- | --- |
| **Subscription Service** | | |
| **Smart Audit Subscription Service** |  | |
| **Smart Test Subscription Service** |  | |
| **Smart Test Modules:** | |
| HCM |  |
| Financials |  |
| Security |  |
| Recruitment |  |

|  |  |
| --- | --- |
| **Subscription Service** | **Subscription Service Charge (annual)\*** |
| **Smart Test** | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| **Smart Audit** | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |

**SMART SUBSCRIPTION SERVICE CHARGES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Summary of Charges** | | | |
| **Services** | **Invoiced** | **Duration** | **Total Charges** |
| The Gold Subscription Service –[Gold Service Description (Up to 4,000)](https://go.kainos.com/rs/272-PGO-379/images/SmartTestGoldServiceDescriptionUpTo4000v3.pdf) | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| [Smart Audit](https://go.kainos.com/rs/272-PGO-379/images/KainosSmartAuditv2Factsheet.pdf)  Subscription Service | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| **REDACTED TEXT under FOIA Section 43 Commercial Interests**. | | | |

\*Subscription Service Charges will increase in line with annual RPI from 1st May 2023.

|  |  |
| --- | --- |
| **Additional Rates - Smart Test** |  |
| Professional Services for Smart Test expansion | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| Professional Services for Smart Audit/Consultancy | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |

1

**Call-Off Schedule 7 (Key Supplier Staff)**

1.1 The Annex 1 to this Schedule lists the key roles (“**Key Roles**”) and names of the

**Annex 1- Key Roles**

|  |  |
| --- | --- |
| **Key Role** | **Contract Details** |
| Client Director – AMS Services | Full-time Permanent |
| Engagement Manager – AMS Services | Full-time Permanent |
| Customer Success Manager – Smart | Full-time Permanent |
| Smart Gold Test/Audit Consultant | Full-time Permanent |
|  |  |
|  |  |

It is agreed and acknowledged:

1. That Supplier personnel providing the services may be substituted by the Supplier with staff of equivalent skills and expertise providing reasonable notice where practicable; and
2. The Supplier personnel remain under the management and control of the Supplier at all times.

**Call-Off Schedule 9 (Security)**

**Part A: Short Form Security Requirements**

**1. Definitions**

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

|  |  |
| --- | --- |
| **"Breach of Security"** | 1. **the occurrence of:**     1. **any unauthorised access to or use of the**   **Deliverables, the Sites and/or any**  **Information and Communication**  **Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or**   * 1. **the loss and/or unauthorised disclosure of any information or data (including the**   **Confidential Information and the**  **Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,**   1. **in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;** |
| **"Security**  **Management Plan"** | **3 the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.** |

1. **Complying with security requirements and updates to them** 
   1. The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.
   2. The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan:

* [https://go.kainos.com/rs/272-PGO-379/images/KainosSmartSecurityProgramv3.pdf](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgo.kainos.com%2Frs%2F272-PGO-379%2Fimages%2FKainosSmartSecurityProgramv3.pdf&data=05%7C01%7CS.Gowdy%40kainos.com%7C1c6e1d5466784534240408da2f55b5c8%7C7ed9bdc7964d4dc09084812b90e05c6d%7C0%7C0%7C637874342413987688%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=kIaUhYNAlVGZss4lCFzUGBhP%2F2r2n6Ddem44YZZWs60%3D&reserved=0)
* [https://go.kainos.com/rs/272-PGO-379/images/KainosAuditSecurityProgramv3.pdf](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgo.kainos.com%2Frs%2F272-PGO-379%2Fimages%2FKainosAuditSecurityProgramv3.pdf&data=05%7C01%7CS.Gowdy%40kainos.com%7C1c6e1d5466784534240408da2f55b5c8%7C7ed9bdc7964d4dc09084812b90e05c6d%7C0%7C0%7C637874342413987688%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=qZwViqojkbqyTxDeB%2FW8722Nz8B9SebRpoJhL3a6xaE%3D&reserved=0)
* [https://go.kainos.com/rs/272-PGO-379/images/kainosWDSecurityProgramfactsheetRHv1.pdf](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgo.kainos.com%2Frs%2F272-PGO-379%2Fimages%2FkainosWDSecurityProgramfactsheetRHv1.pdf&data=05%7C01%7CS.Gowdy%40kainos.com%7C1c6e1d5466784534240408da2f55b5c8%7C7ed9bdc7964d4dc09084812b90e05c6d%7C0%7C0%7C637874342413987688%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=TvBIeu%2B557hSQoup%2FbL%2BnQ3rB7aK%2Fh%2FJcFuvLbH5AhY%3D&reserved=0)

Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy. (Please see Annex B)

* 1. Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.
  2. If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.
  3. Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

1. **Security Standards** 
   1. The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.
   2. The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:
      1. is in accordance with the Law and this Contract;
      2. as a minimum demonstrates Good Industry Practice;
      3. meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and
      4. where specified by the Buyer in accordance with paragraph 2.2 complies with the Buyers Security Policy and the ICT Policy.
   3. The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.
   4. In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.
2. **Security Management Plan** 
   1. **Introduction** 
      1. The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.
   2. **Content of the Security Management Plan** 
      1. The Security Management Plan shall:
         1. comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;
         2. identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
         3. detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer’s Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that

Information, data and/or the Deliverables;

* + - 1. be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer’s Confidential

Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

* + - 1. set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the

Deliverables comply with the provisions of this Contract;

* + - 1. set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and
      2. be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.
  1. **Development of the Security Management Plan** 
     1. Within twenty (20)Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.
     2. If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.
     3. The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph

4.3.2. However a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

* + 1. Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.
  1. **Amendment of the Security Management Plan** 
     1. The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:
        1. emerging changes in Good Industry Practice;
        2. any change or proposed change to the Deliverables and/or associated processes;
        3. where necessary in accordance with paragraph 2.2, any change to the Security Policy;
        4. any new perceived or changed security threats; and
        5. any reasonable change in requirements requested by the Buyer.
     2. The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and

amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation: a) suggested improvements to the effectiveness of the Security

Management Plan;

* + - * 1. updates to the risk assessments; and
        2. suggested improvements in measuring the effectiveness of controls.
    1. Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.
    2. The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

1. **Security breach** 
   1. Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.
   2. Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:
      1. immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

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

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

Breach of Security;

prevent an equivalent breach in the future exploiting the same cause failure; and

as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or

attempted Breach of Security, including a cause analysis where required by the Buyer.

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

**Call-Off Schedule 14 (Service Levels)**

The Services contained as part of the contract includes the following

* Workday AMS
* The provision of the Kainos Smart Test Subscription Service
* Kainos Smart Audit Suscription Service

**AMS Service Hours**

UK: Monday to Friday 0900-1700 GMT Excluding UK public holidays\*

\*Bank holidays are not classified as public holidays

**Incident Logging procedure and Service Desk number**

Incidents should be logged by the Customer through the relevant Supplier incident management application. In addition to raising an incident on the application, although not required, the Customer may also contact the Kainos Service Desk on **REDACTED TEXT under FOIA Section 40, Personal Information**.

The following Target Response and Resolution Times and Incident Classifications apply to the provision of the **AMS Service:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Priority** | **Classification** | **Description & Examples** | **Target Response Time(s)** | **Target Resolution Time(s)\*** | |
| Critical | High Impact & High Urgency | Business critical integration or software functionality not usable for any purpose; | 1 hour | 2 hours | |
| Data inaccuracies impacting all Workday users; |
| All users affected; |
| Unable to proceed and creating major business impact. |
| High | High Impact & Medium Urgency; | Malfunction impacting important integration or software functionality; | 2 hours | 4 hours | |
| Medium Impact & High Urgency | Business process, absence plan, benefits plan or similar isn’t completing; |
|  | Majority of users affected. |
| Medium | High Impact & Low Urgency; | Malfunction impacting standard integration or software functionality; | 4 hours | 12 hours | |
| Medium Impact & Medium Urgency | Business process, absence plan, benefits plan or similar creating an issue, but workaround available; |
| Low Impact & High Urgency | Multiple users affected. |
| Low | Medium Impact & Low Urgency | Malfunction impacting non-critical integration or software functionality; | 1 day | 3 days | |
| Low Impact & Medium Urgency | Business process, absence plan, benefits plan or similar requires amending, but not blocking progress; |
|  | Single user affected or multiple users inconvenienced. |
| Minor | Low Impact & Low Urgency | Minor issue inconveniencing users; | 2 days | Target resolution time provided with each ticket raised | |
| No impact on business; |
| Cosmetic modification; |
| Usability suggestion. |
| Query | Request for advice, guidance or information | Request for investigation into behaviour of functionality; | 2 days | Target resolution time provided with each ticket raised | |
| Request for instructions or guidance on how to achieve outcome. |
| Service Request | Standard change that does not require approval | Password reset; | 2 days | Target resolution time provided with each ticket raised | |
| Set up of new incident management application user. |
| Problem | Investigation of underlying root cause of 1 or more Incidents | Grouping of one or more Incidents with similar symptoms to investigate and resolve underlying root cause. | 2 days | Target resolution time provided with each ticket raised | |
| Change Request | Request for change or enhancement | Introduction of new functionality; | 2 days | Target resolution time and estimated cost will be provided by the supplier in response to each ticket raised | |
| Enhancement of existing functionality. |
| \*The Target Resolution time will stop when the incident is with the Buyer or a Third Party for input or investigation, which is reasonably necessary to resolve the incident. | | | | |
| The target resolution time will resume when the third party has provided input sufficient to enable the Supplier to progress resolution of the incident. | | | | |
| All target resolution time metrics will be recorded by the Supplier and provided to the Buyer on request. | | | | |

AMS Buyer Dependencies:

|  |
| --- |
| The Buyer will: |
| * provide 1st and 2nd Tier Support, this involves:   + performing initial investigation and assessment of Incidents (to include liaising with Customer users to obtain all the relevant detail and error analysis information);   + resolving straightforward issues and Incidents (for example and without limitation, data issues or simple configuration changes);   + logging Incidents requiring more detailed investigation and providing a full description and information in the Kainos incident management application);   + prioritising Incidents based on the Incident classifications set out in the Statement of Work;   + providing interface between 3rd and 4th Tier Support and Customer users and providing Incident feedback and appropriate workarounds to Customer users;   + keeping informed of Workday Updates and supply details to Customer users on new features;   + facilitating testing of changes on non-Production environment;   + scheduling changes that need to be applied by Kainos to the production system (once testing has been confirmed as successful);   + managing Third Party Software supplier relationships and the notification of changes to Kainos (via the Kainos incident management application) of any Third Party Software systems to allow Kainos to impact assess the changes on the Workday Service;   + close Incidents; * support any software or equipment with which the Supported Items or Workday Service interacts; * liaise directly with Workday for resolution of Workday Service issues; * ensure Workday Update regression test activities are planned and executed in timely manner; * fulfil its obligations under the Statement of Work. * ensure that data (including Personal Data) required for the Services is only provided to Kainos via agreed and secure means (typically via sFTP * not submit data files (including Personal Data) required for the Services to Kainos via email or other solutions not intended for this purpose, including Teamwork and Jira (even if password protected) * ensure that all data (including Personal Data) is removed from the sFTP (or other agreed Customer solution) when it is no longer required provided that where Kainos provides the mechanism for data transfer, it (not the Customer) will be responsible for the deletion of data when it is no longer required. |

**SMART TEST & AUDIT SUBSCRIPTION SERVICE – SLA**

(In this section, references to the “Customer” should be read as references to the Buyer and references to "Kainos” should be read as references to the Supplier.

Text

Description automatically generated

**Call-Off Schedule 20 (Call-Off Specification)**

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

Full details of the requirements are as below.

1. Application Management Services (“AMS”), a Workday Support Service.

|  |  |
| --- | --- |
| The AMS Support required: | |
| Service Management | An available named Service Manager to:   * assess and manage AMS. * respond to requests for service within the SLA and progress appropriately. * provide consultancy. * set up and on-going access to the supplier incident management application for the Customer including Incident history and traceability until completed investigation. * monthly MI reporting. * quarterly service reviews. |
| Telephone Advice and Assistance | To address Customer enquiries in respect of the use or operation of the Supported Items during the Service Hours, within the Service Period. |
| Reporting Services | * the provision of status updates by the supplier to the Customer in the form of monthly status reports detailing Incidents raised. * SLA metrics. * any potential recommendations or AMS improvements. * quarterly status meetings with the Customer to review the AMS. |
| 3rd and 4th Tier Support | * provision of temporary or permanent corrections to the Supported Items where Incidents have been escalated from 1st and 2nd Line Tier (and where approval has been provided) to implement changes that cover:   + test of correction or changes on the client non-Production environment; and   + deployment of correction or change to the Production environment. * qualified personnel to provide support during the Service Hours and investigate Incidents with the Supported Items. * provision of consultancy services to Customer’s 1st and 2nd Tier Support (if required); * provision of estimates on the length of time to correct Incidents. * investigation and assessment of any Third Party Software changes and the possible impact on the Workday Service with recommended actions. * augment Customer support teams with supplier AMS staff (if required); * deliver configuration review and optimisation programmes (if required). |

**AMS Supported Items**

The supplier will support the following items for all Modules deployed by the Customer during the Service Period:

* Workday Configurations
* Workday Business process and security
* Workday Integrations
* Workday Custom Reports

Collectively the Application Management Services (“**AMS”**).

**Additional Services**

The Customer may procure the following additional Services under this Order Form, at any time during the Service Period as further set-up at Schedule 5 above.

1. **Smart Test Gold Subscription Service**

The software as a service (SaaS) application known as Smart Test is a cloud-based, automated testing product for Workday implementations and the associated support. The functionality of Smart Test is dependent on the service type (Gold) and the Modules as set out below.

The Smart Test Gold Subscription Service provides the following:

* Execute Each Baseline test pack on Sandbox only
* Providing Reports to SLC on a weekly basis
* Facilitating Gold Service Review
* Updating tickets in Smart Issue Tracker
* Providing MI on Smart Metrics and providing as part of Quarterly Business Review process
* Annual GAP Analysis

For the following four modules:

* HCM
* Security
* Financials
* Recruitment

Professional Services – This will be required on an ad hoc basis for related project work.

1. **Smart Audit Subscription**

Smart Audit is a Software as a Service Offering designed to highlight potential risks in Customer’s Workday configuration by identifying instances of specific, pre-defined scenarios in one or more Workday tenant/s. Audit looks at a Customer’s Workday Tenant configurations and identifies potential risk ‘Cases’ in certain scenarios - “Audit Checks”.

Audit comes with a bank of Audit Checks and provides Customers with mechanisms to create new Audit Checks. New Audit Checks may also be added by Kainos from time to time.

Kainos Audit includes a workflow to help Customers manage Cases.

**Key Functionality:**

**Access Monitoring:**

• Data Access - Kainos Audit will provide Audit Checks to monitor access to named fields (data elements) in Workday after which Kainos Audit will provide a list of Workday users or security groups (each represented as a Case) with access to the specified field/s.

• Business Process and Task Access - Kainos Audit will provide Audit Checks to monitor access to named Business Processes or Tasks in Workday after which Kainos Audit will provide a list of Workday users or security groups (each represented as a Case) with access to the specified Business Processes or Tasks.

**Activity Monitoring:**

• Worker View Access - Kainos Audit will provide Audit Checks to monitor user activity against other workers in Workday tenants.

• Change to Tenant configuration - Kainos Audit will provide Audit Checks to monitor changes to certain elements of tenant configuration.

**Additional Services**

The Customer may procure the following additional Services under this Order Form, at any time during the Service Period (or agreed extensions to it):

1. Smart professional services

2. Ad-Hoc professional services (Project Work)

**Call-Off Schedule 23 (Supplier-Furnished Terms)**

**Part 1A Non-COTS Third Party Software**

Not applicable – Annex 1

**Part 1B COTS Software**

Not Applicable – Annex 2

**Part 1C Software as a Service (SaaS) Terms**

Terms for provision of the Smart Test and Audit Software as a Service solutions are detailed here:.

https://go.kainos.com/rs/272-PGO-379/images/SubscriptionServiceTermsofUsev5.pdf

**Part 1D Software Support and/or Maintenance Terms**

Terms for provision of the AMS Software Support and/or Maintenance services are detailed here:

https://go.kainos.com/rs/272-PGO-379/images/WorkdayServicesTermsv7.pdf